secure elements®

Audit. Evaluate. Comply.

"It really is that simple"

2nd Annual Security Automation Conference and Workshop

Andrew Bove
CTO, Secure Elements, Inc.
Above@Secure-Elements.com

DISA

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

NIST

Agenda

1. Background
2. Our Context -- “Codification”
3. Deriving, Composing and Refining xContent
   - Auditing
   - Vulnerability Scanning
4. Application
5. Results

Secure Elements Company Overview

Secure Elements at a glance …

- Secure Elements is dedicated to developing innovative products to evolve the way organizations achieve IT security and compliance
- We enable organizations to ***audit, evaluate, and comply*** with internal, industry, and regulatory policies

- Venture Capital Funded
  - Carlyle Venture Partners
  - DCM - Doll Capital Management
- Founded 2003
- Headquarters in Herndon, Virginia
  - Regional US sales offices
  - Strong industry & channel partners

- C5 Security Solutions
  - C5 Enterprise Vulnerability Management Suite
  - C5 Alert Service
  - C5 Enterprise Security Portal
- Markets Served
  - Government
  - Finance, Healthcare, Energy
  - Critical Infrastructure Providers

Industry Alliances:

redhat. bmcsoftware Google Internet Security Systems Microsoft Cisco Systems Juniper ORACLE IBM SAIC From Science to Solutions™

C5 Enterprise Vulnerability Management - Features

Audit

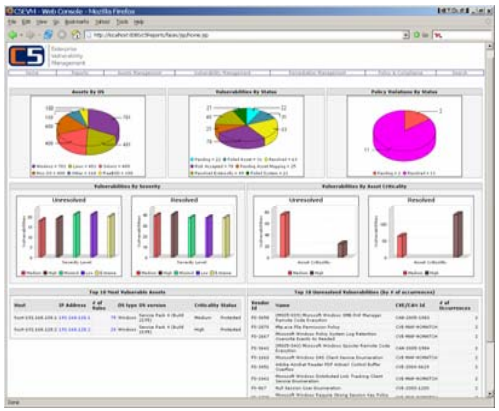
- ❑ Asset inventory on-demand
- ❑ Security vulnerabilities & exposures
- ❑ Compliance score by asset

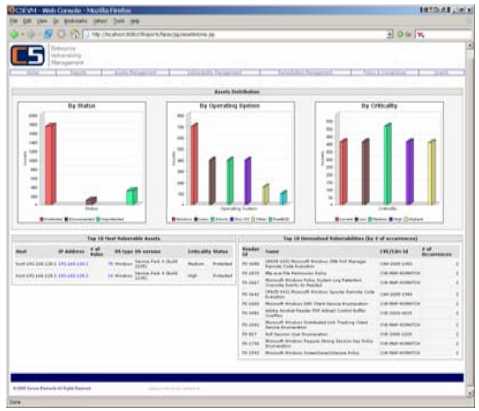
Evaluate

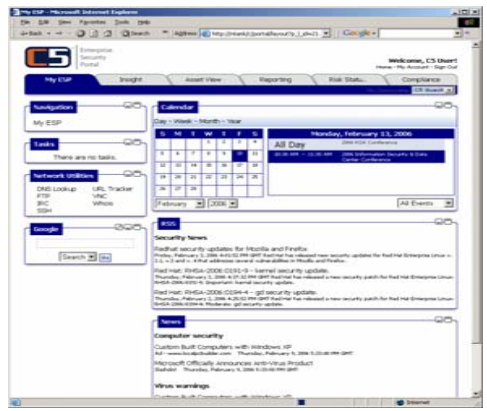
- ❑ Enterprise security status
- ❑ Compliance score by department
- ❑ Asset criticality vs. risk exposure

Comply

- ❑ Corporate policies
- ❑ Regulated & industry specific
- ❑ Standards & best practices







Appreciation

"The hardest part of building a software system is deciding what to build." - Fred Brooks

- Many Sources of Knowledge
  - Microsoft Windows Security Resource Kit
  - http://www.securityfocus.com/
  - http://sans.org (SANS Top 20)
  - FISMA
  - SOX
  - CIS
  - HIPPA
- Very Little is Action-able at an Enterprise level

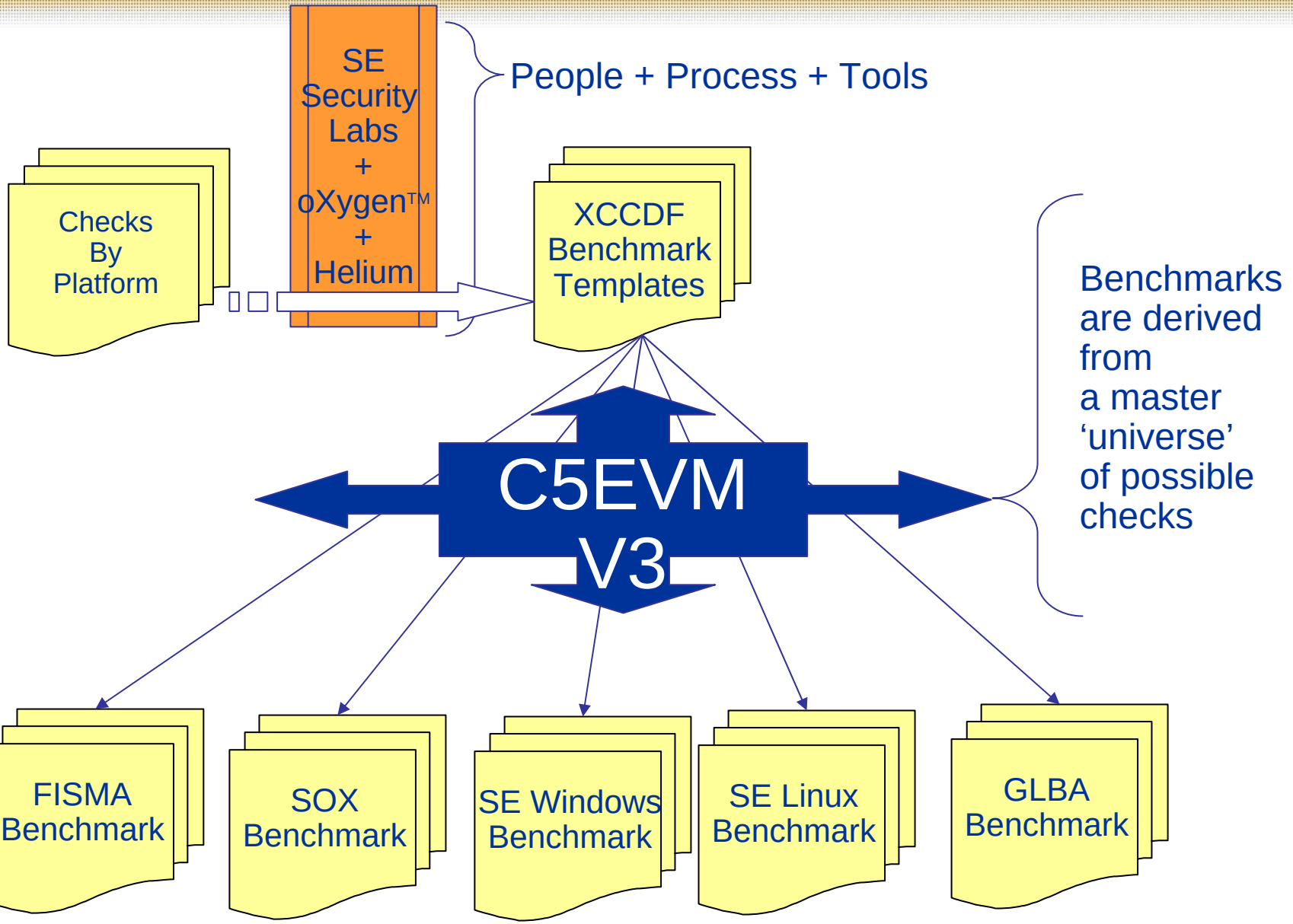
Codification - Checks by Platform

Local Security Policy Settings	WinXP Standalone	WinXP Domain	Win2003 Standalone	Win2003 Domain	WinSrv2000 Standalone	WinSrv2000 Domain	WinPro2000 Standalone	WinPro2000 Domain
Account Policies								
Password Policy								
Enforce password history	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password length	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password must meet complexity requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Store passwords using reversible encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Account Lockout Policy								
Account lockout duration	Yes	Yes	Yes	Yes				Yes
Account lockout threshold	Yes	Yes	Yes	Yes				Yes
Reset account lockout counter after	Yes	Yes	Yes	Yes				Yes
Local Policies								
Audit Policy								
Audit account logon events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes	Yes	Yes		
Audit directory service access	Yes	Yes	Yes	Yes	Yes	Yes		
Audit logon events	Yes	Yes	Yes	Yes	Yes	Yes		
Audit object access	Yes	Yes	Yes	Yes	Yes	Yes		
Audit policy change	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit privilege use	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit process tracking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit system events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Right Assignment								
Access this computer from Network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Act as a apart of the operating system	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Add workstations to domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adjust memory quotas for a process	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on locally	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on through Terminal Services	Yes	Yes	Ye				N/A	N/A
Backup files and directories	Yes	Yes	Ye				Yes	Yes
Bypass traverse checking	Yes	Yes	Ye				Yes	Yes
Change the system time	Yes	Yes	Yes				Yes	Yes
Create a pagefile	Yes	Yes	Yes		Yes	Yes	Yes	Yes
Create a token object	Yes	Yes		Yes	Yes	Yes	Yes	Yes
Create global objects	SE	SE	SE	SE	SE	SE	SE	SE
Create permanent shared objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Debug programs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny access to this computer from the netwo	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a batch job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on locally	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A

An OVAL Check Exists

SE Produced ~400

Evolution of a XCCDF Benchmark



C5 Command Center

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Search Favorites

Address https://10.2.2.11/CommandCenter/faces/jsp/home.jsp

Google Search 12 blocked Check AutoLink AutoFill Options

Enterprise Vulnerability Management

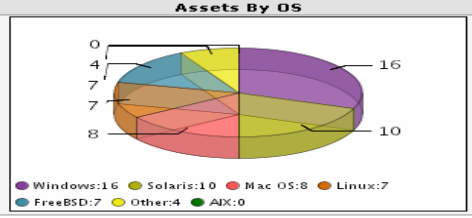
Welcome c5evm_admin

Logout

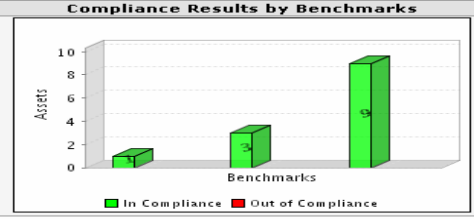
RSS security feed

Home | Compliance | Reports | Assets Management | Vulnerability Management | Remediation Management

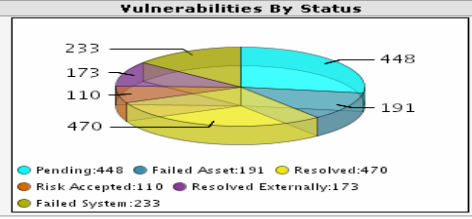
Assets By OS



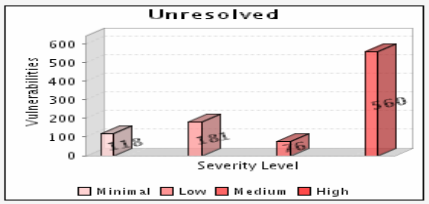
Compliance Results by Benchmarks



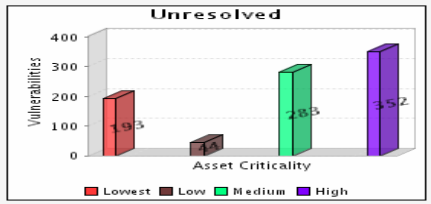
Vulnerabilities By Status

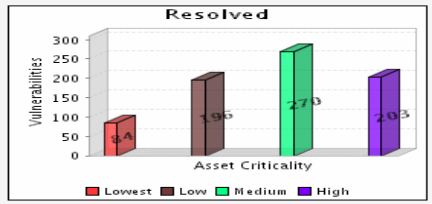


Vulnerabilities By Severity



Vulnerabilities By Asset Criticality





Top 10 Most Vulnerable Assets

Export to Pdf

Host	IP Address	# of Vulns	OS type	OS version	Criticality	Status
SOJA-ORACLE	10.0.10.171	165	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Protected
W2K3SSP0O2K31-3	10.2.243.248	138	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Lowest	Protected
W2K3SSP0O2K31-2	10.2.232.235	132	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Medium	Protected
W2KPRO-SP4-VM2	10.2.251.221	118	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Disconnected
W2KASRV-SP4-VM2	10.2.251.230	77	Microsoft Windows 2000 Advanced Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KSRV-SP4-VM2	10.2.248.237	50	Microsoft Windows 2000 Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KPRO-SP3-VM3	10.2.231.229	49	Microsoft Windows 2000 Professional	Service Pack 3 (Build 2195)	Lowest	Protected
W2KPRO-SP2-VM2	10.2.254.213	46	Microsoft Windows 2000 Professional	Service Pack 2 (Build 2195)	High	Protected
W2KPRO-SP4-VM3	10.2.242.214	30	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	Low	Protected
W2KSRV-SP3-VM2	10.2.241.246	24	Microsoft Windows 2000 Server	Service Pack 3 (Build 2195)	Medium	Protected

Top 10 Unresolved Vulnerabilities (by # of occurrences)

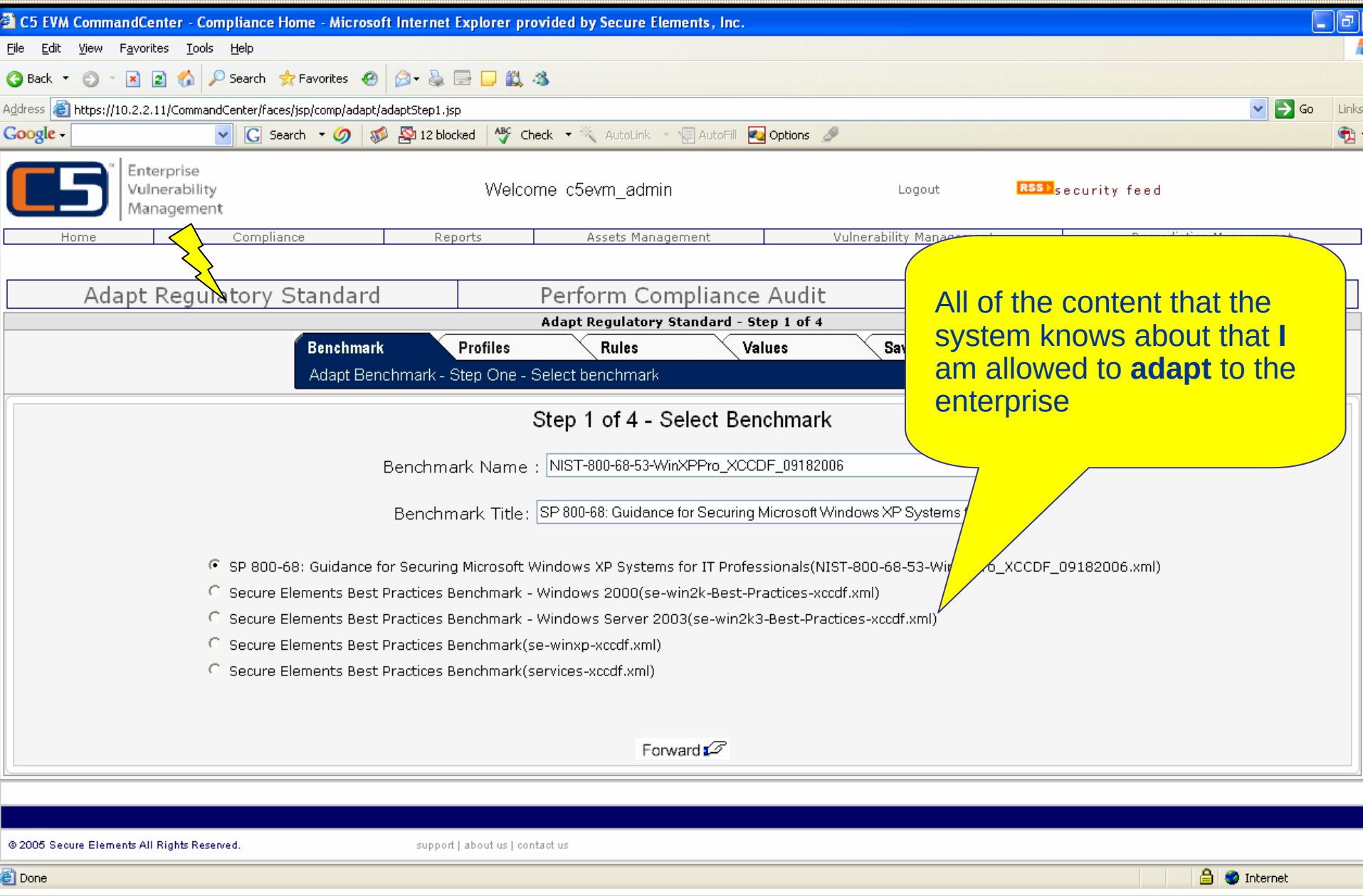
Export to Pdf

Vendor Id	Name	CVE/CAN Id	Severity	# of Occurrences
oval:org.mitre.oval:def:115	Hyperlink Object Function Vulnerability	CVE-2006-3438	High	10
oval:org.mitre.oval:def:13	Buffer Overrun in HTML Help Vulnerability	CVE-2006-3357	High	8
oval:org.mitre.oval:def:155	User Profile Elevation of Privilege Vulnerability	CVE-2006-3443	High	8
oval:org.mitre.oval:def:21	Microsoft Office Remote Code Execution Using a Malformed GIF Vulnerability	CVE-2006-0007	High	8
oval:org.mitre.oval:def:492	Buffer Overrun in Server Service Vulnerability	CVE-2006-3439	High	8
oval:org.mitre.oval:def:841	Unhandled Exception Vulnerability	CVE-2006-3648	High	8
oval:org.mitre.oval:def:1559	Windows Media Player Plug-in EMBED Vulnerability	CVE-2006-0005	Medium	8
oval:org.mitre.oval:def:723	DNS Client Buffer Overrun Vulnerability	CVE-2006-3441	High	7
oval:org.mitre.oval:def:747	Winsock Hostname Vulnerability	CVE-2006-3440	High	7
oval:org.mitre.oval:def:999	Hyperlink Object Buffer Overflow Vulnerability	CVE-2006-3086	High	7

support | about us | contact us

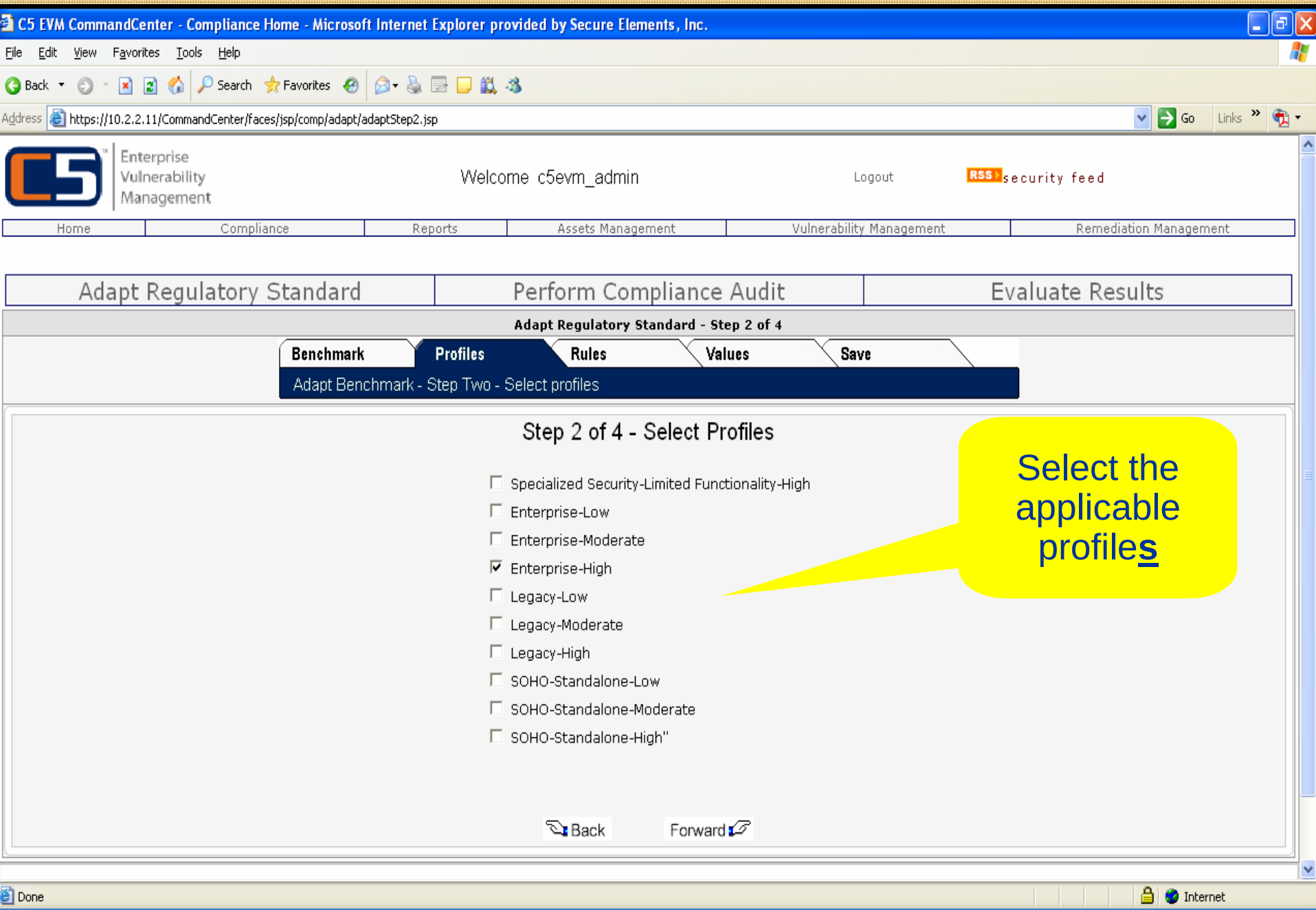
Internet

Deriving Benchmarks Through Adaptation



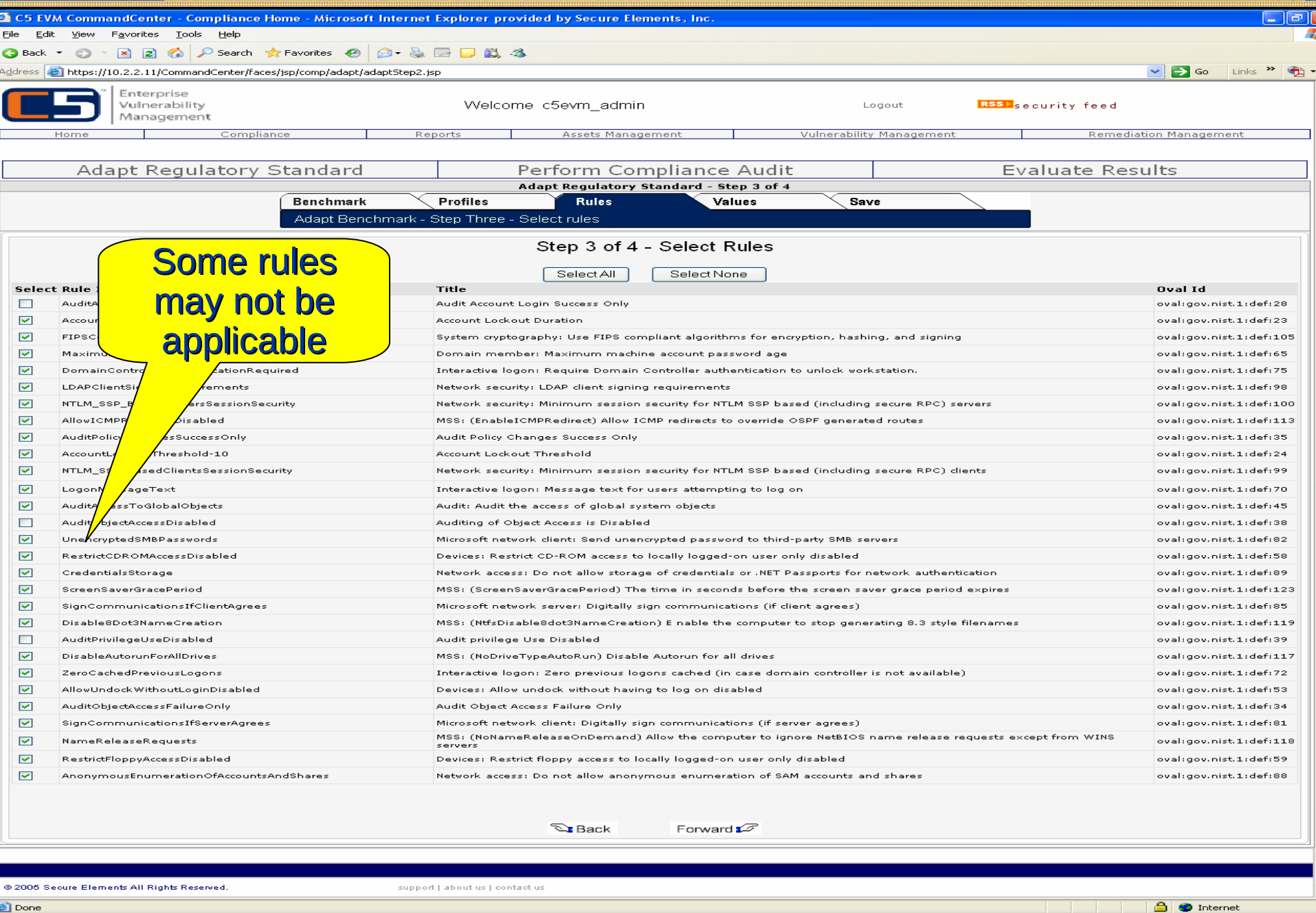
All of the content that the system knows about that **I** am allowed to **adapt** to the enterprise

Adaptation of the NIST Benchmark

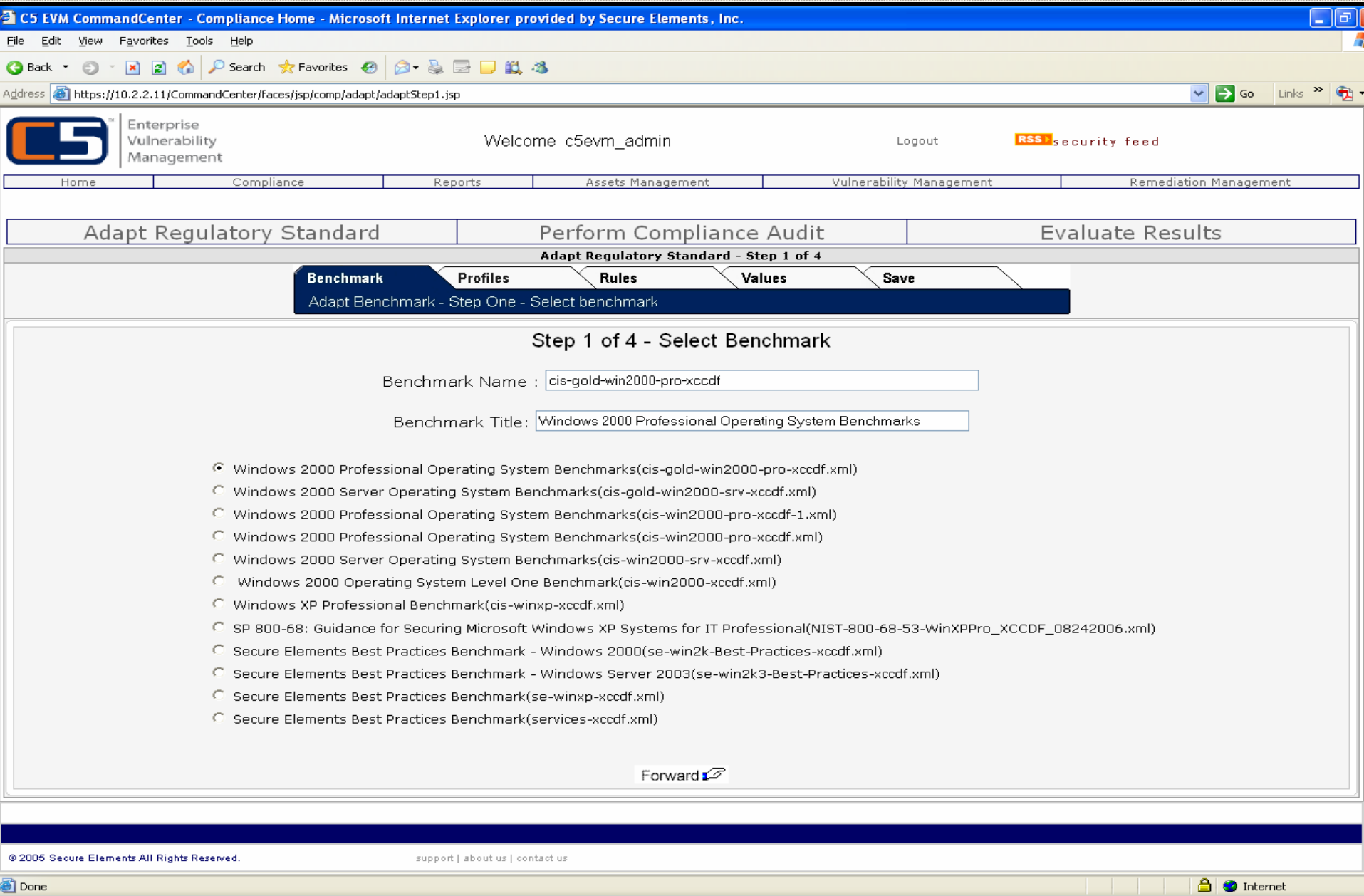


Select the applicable profiles

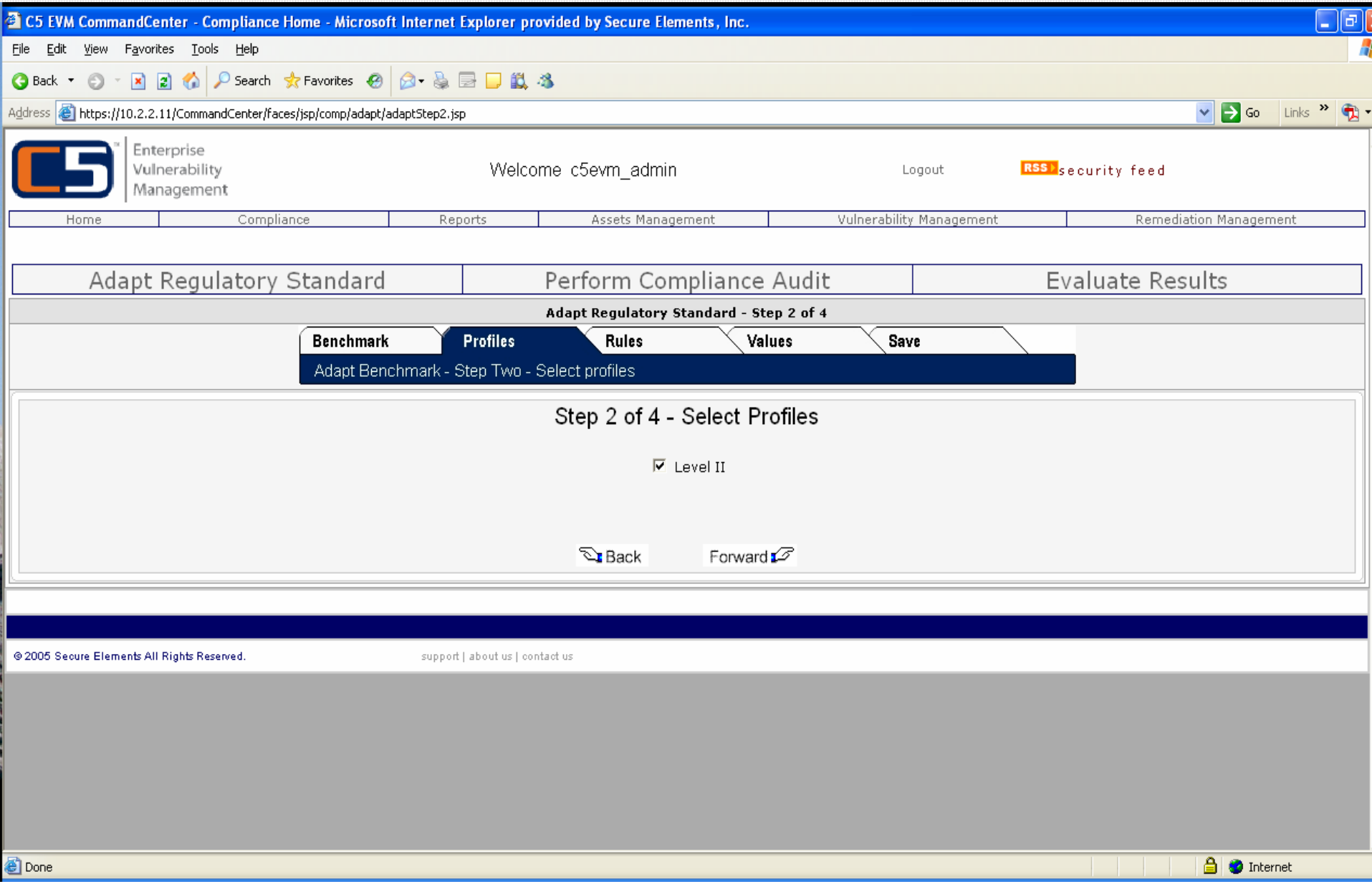
Adaptation of the NIST Rules



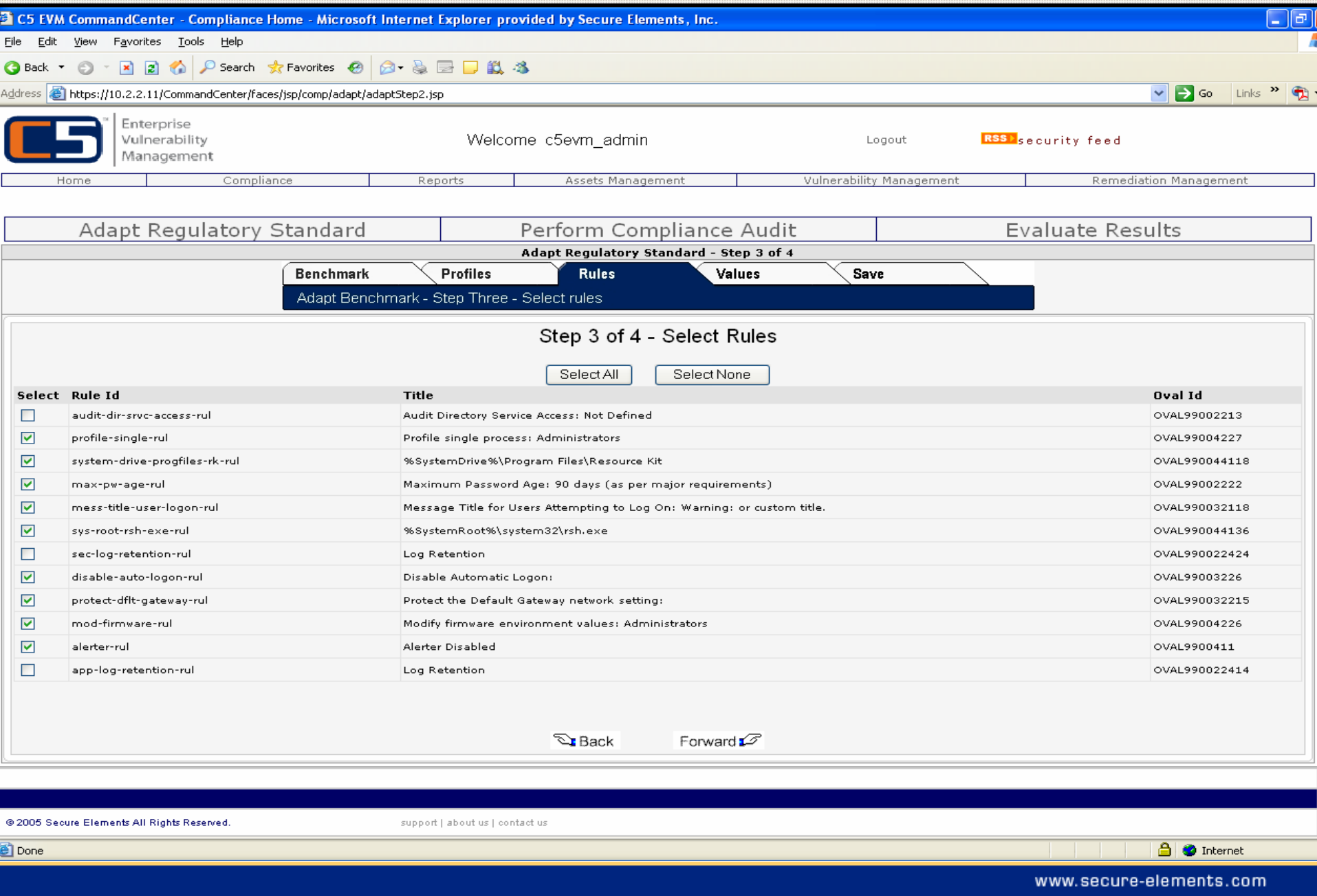
Adaptation of the CIS Benchmark



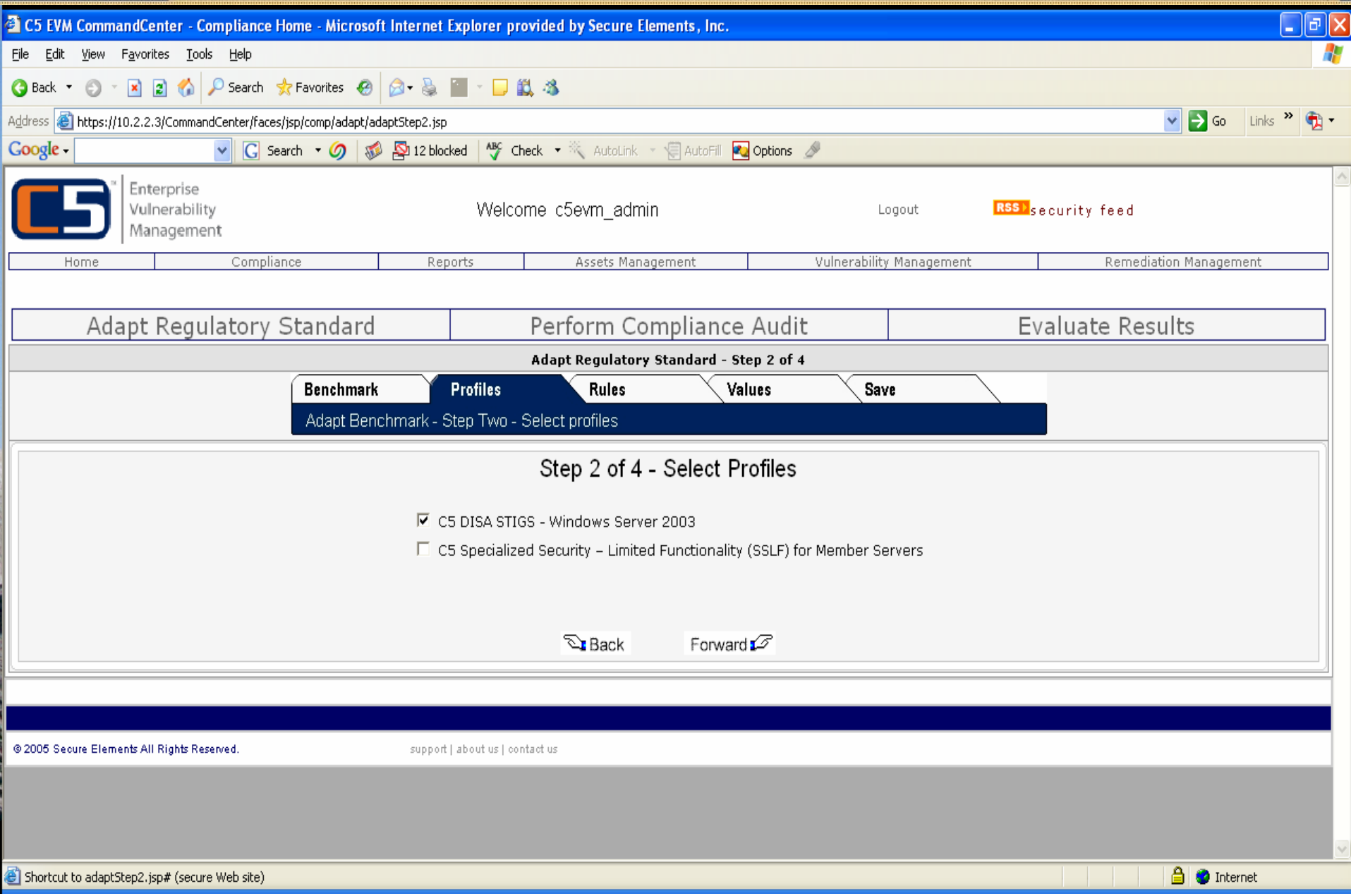
Adaptation of the CIS Rules



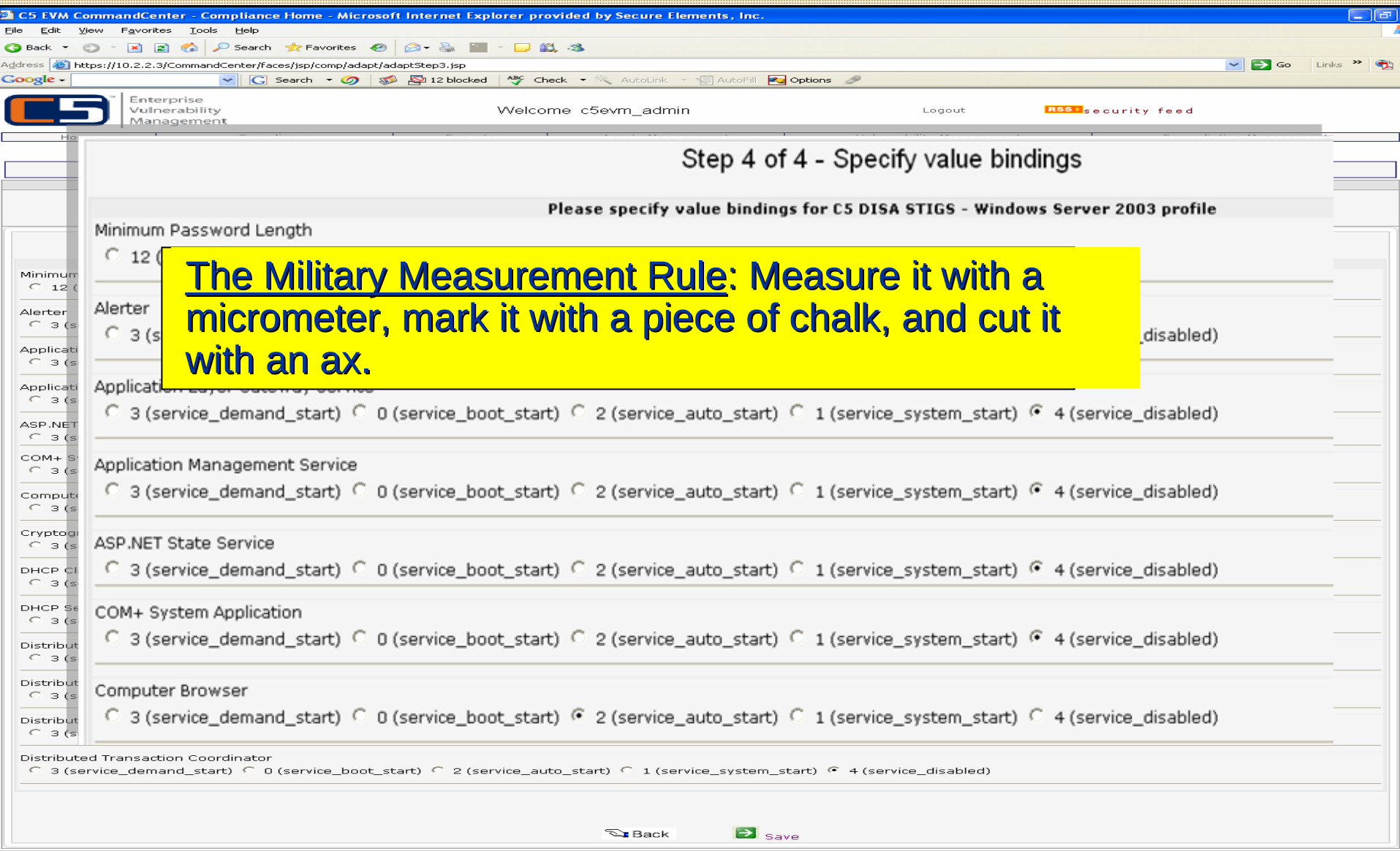
Adaptation of the CIS Rules



Adaptation of the C5 STIGS

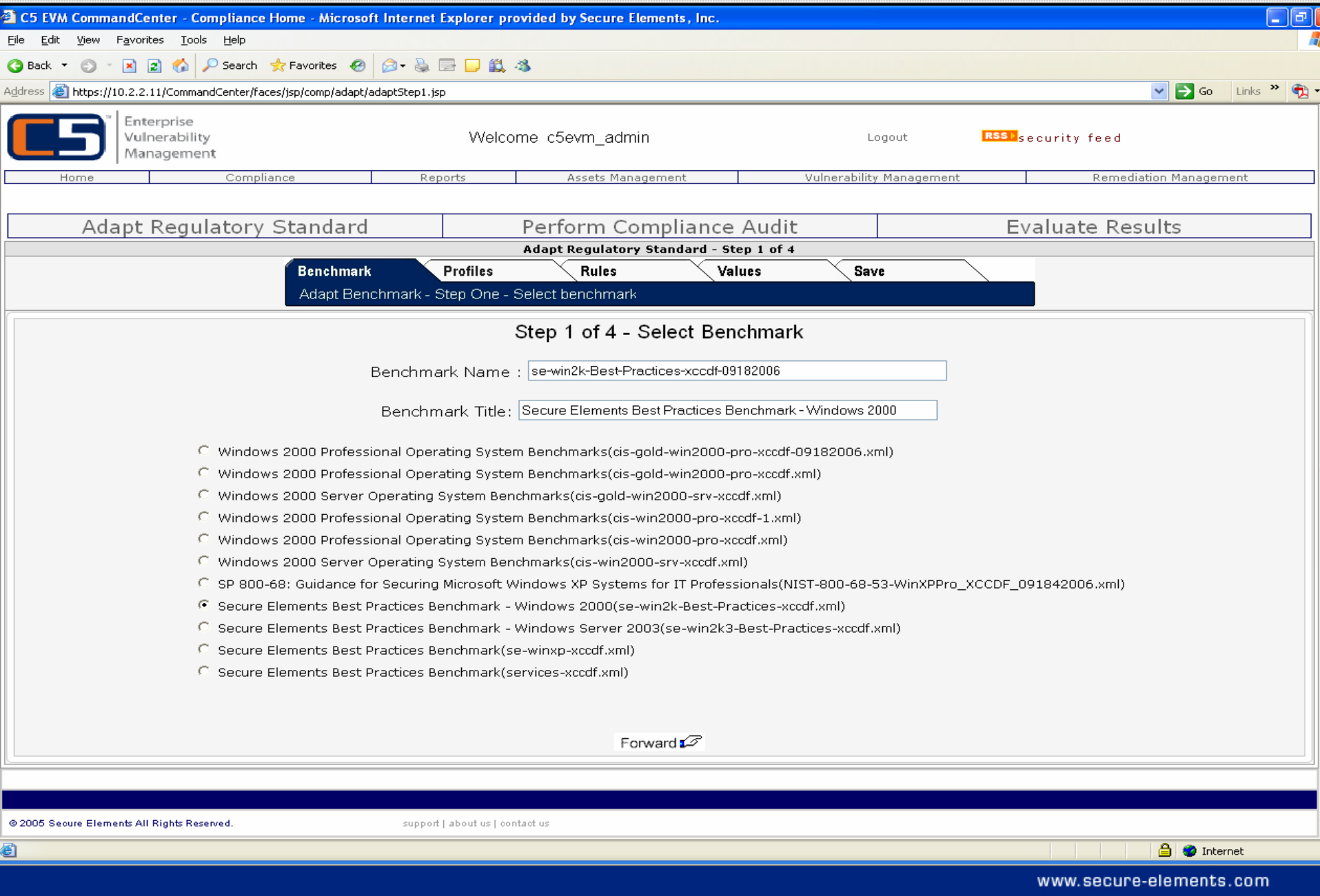


Adaptation of Tolerance of Rules

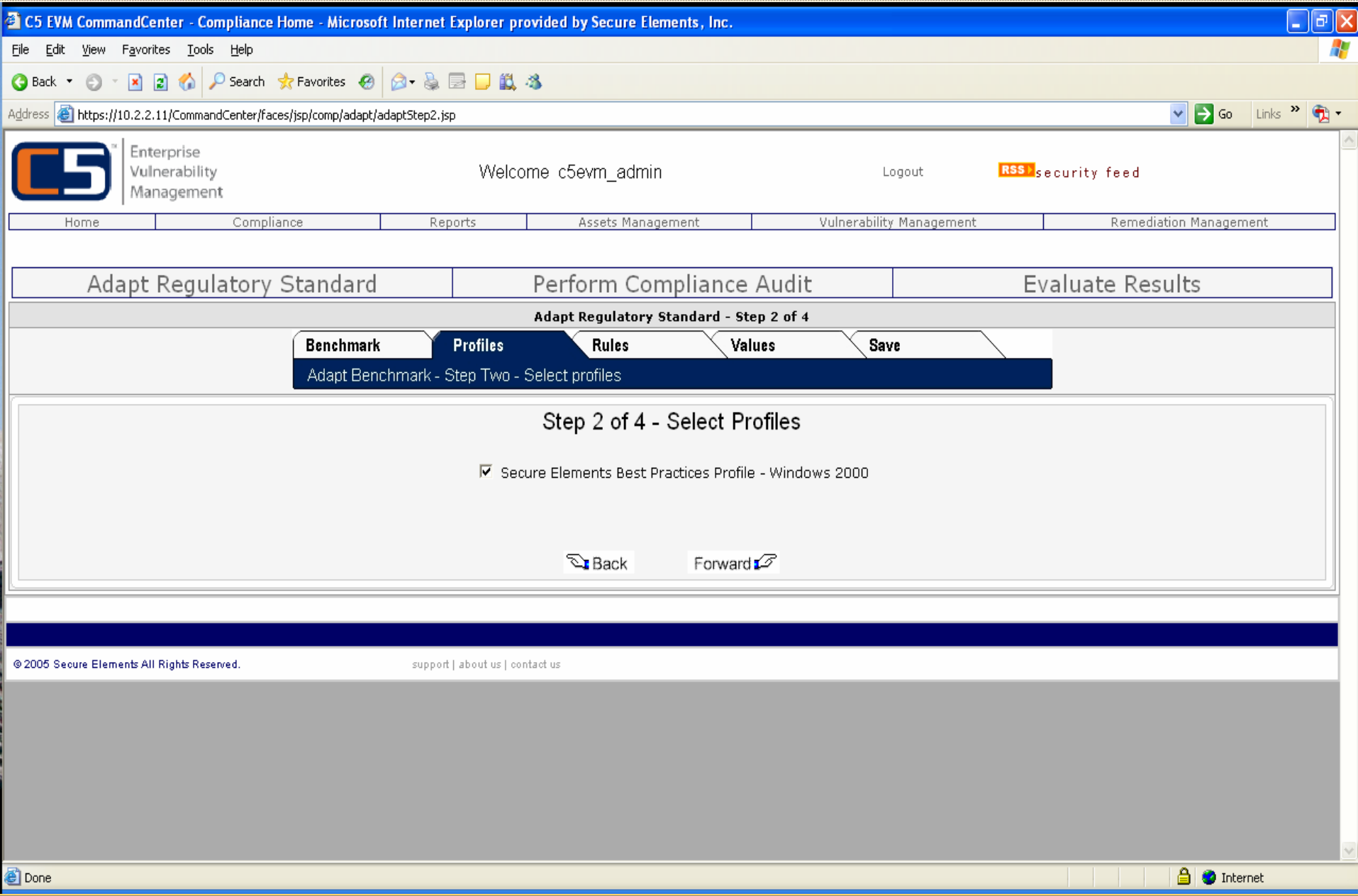


The Military Measurement Rule: Measure it with a micrometer, mark it with a piece of chalk, and cut it with an ax.

Adaptation of the Secure Elements Benchmark



Adaptation of the Secure Elements Profiles



Adaptation of the Secure Elements Rules

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Address https://10.0.10.179/CommandCenter/faces/jsp/adaptStep3.jsp

Enterprise Vulnerability Management

Welcome c5evm_admin Logout RSS security feed

Home | Compliance | Reports | Assets Management | Vulnerability Management | Remediation Management

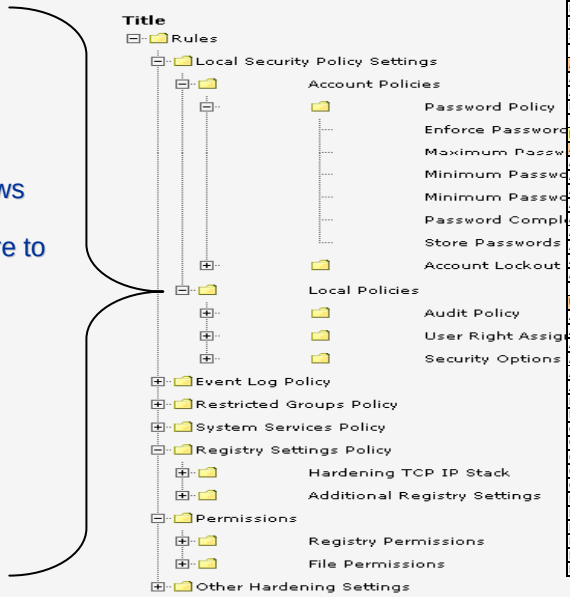
Adapt Regulatory Standard | Perform Compliance Audit | Evaluate Results

Adapt Regulatory Standard - Step 3 of 4

Benchmark | Profiles | Rules | Values | Save

Adapt Benchmark - Step Three - Select rules

Leveraging indexing allows us to provide more structure to the content



Local Security Policy Settings	WinXP Standalone	WinXP Domain	Win2003 Standalone	Win2003 Domain	WinSrv2000 Standalone	WinSrv2000 Domain	WinPro2000 Standalone	WinPro2000 Domain
Account Policies								
Password Policy								
Enforce password history	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password length	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password must meet complexity requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Store passwords using reversible encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Account Lockout Policy								
Account lockout duration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Account lockout threshold	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reset account lockout counter after	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local Policies								
Audit Policy								
Audit account logon events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit privilege use	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit process tracking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit system events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Right Assignment								
Access this computer from Network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Act as a apart of the operating system	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Add workstations to domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adjust memory quotas for a process	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on locally	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Backup files and directories	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bypass traverse checking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Change the system time	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create a pagefile	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create a token object	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create global objects	SE	SE	SE	SE	SE	SE	SE	SE
Create permanent shared objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Debug programs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny access to this computer from the network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a batch job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on locally	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A

group

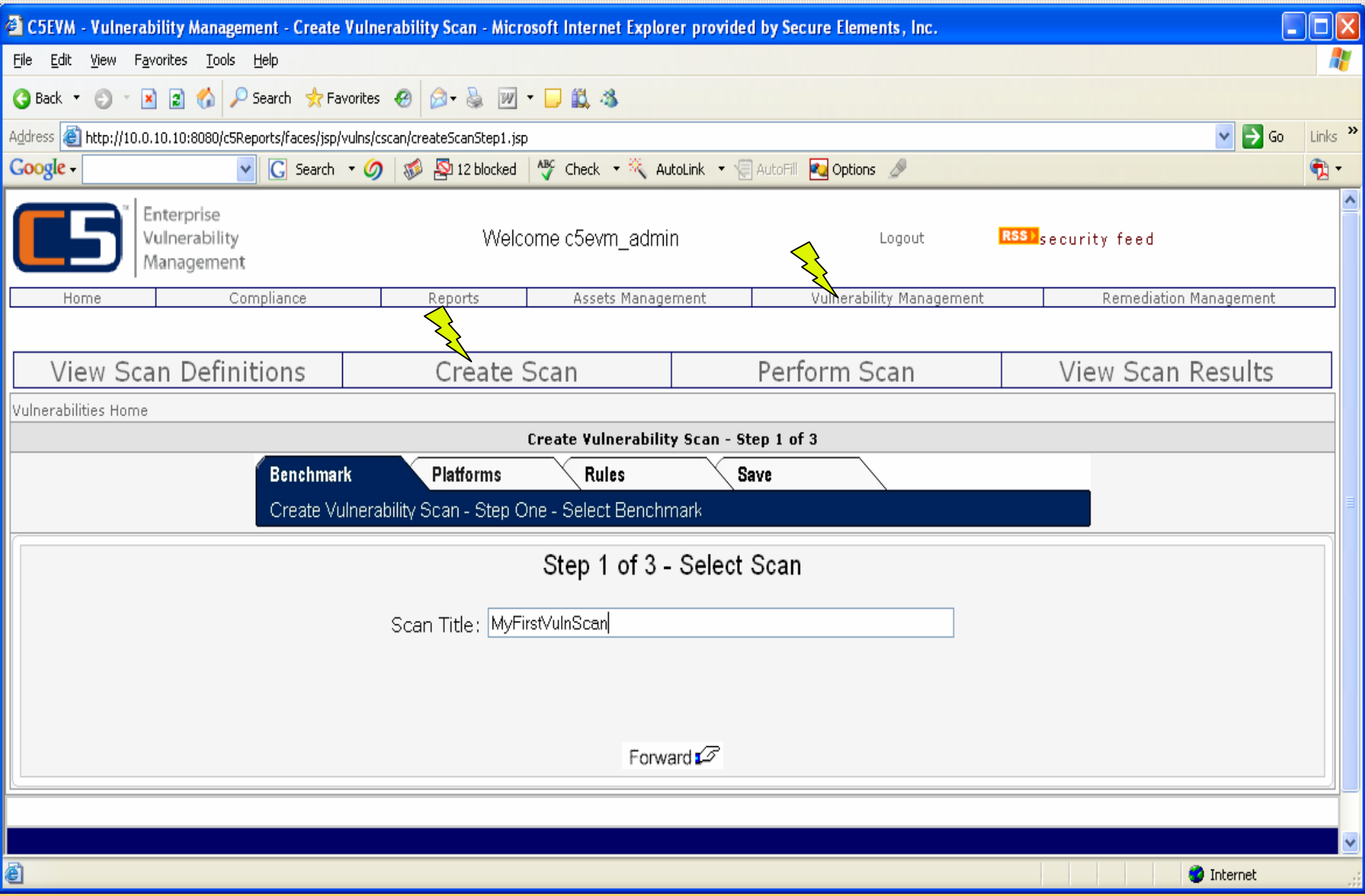
Back Forward

support | about us | contact us

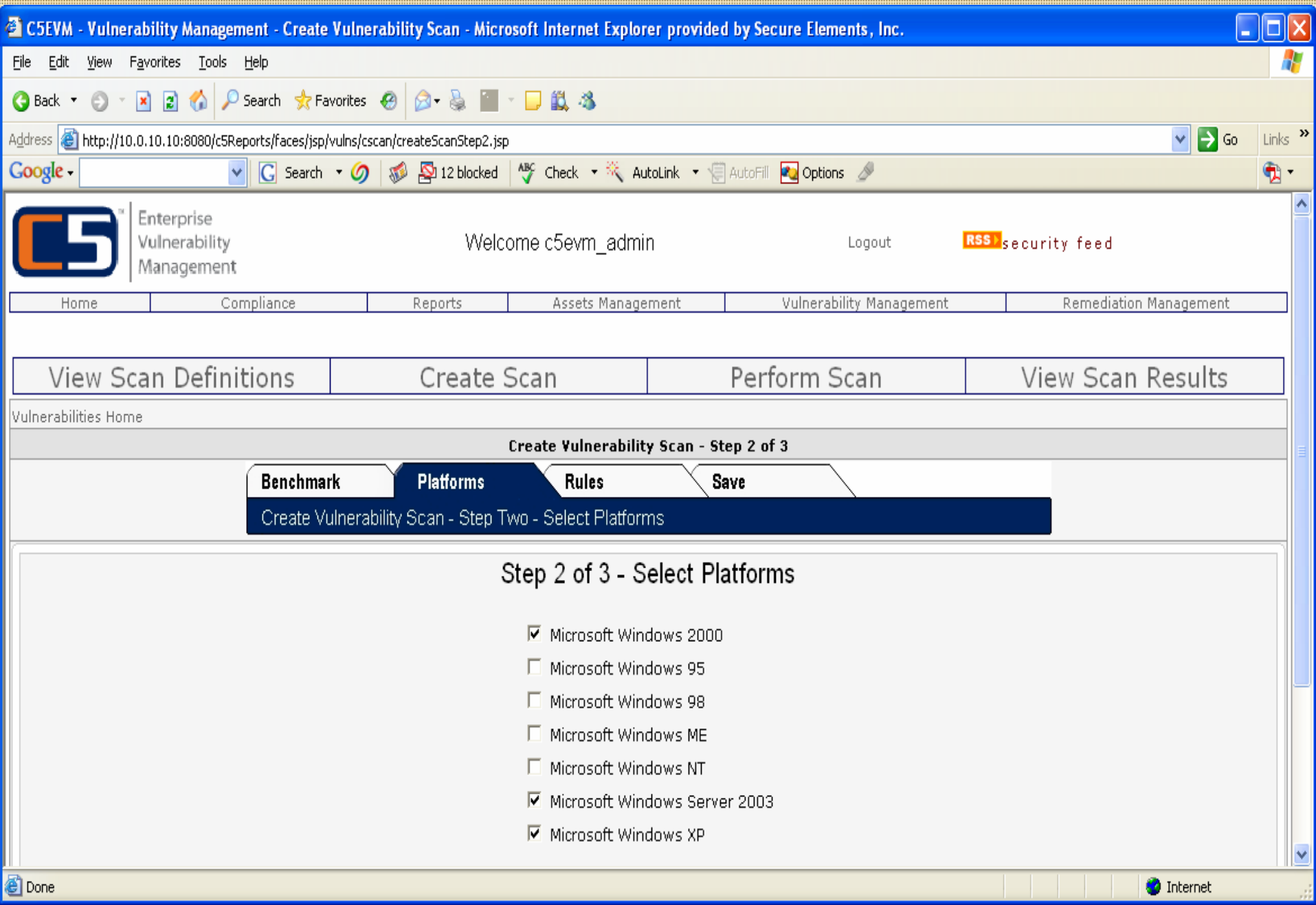
Internet

- XCCDF Allows grouping of OVAL Compliance Tests
- Why Not Group OVAL Vulnerability Tests into a Vulnerability “Job” using XCCDF?

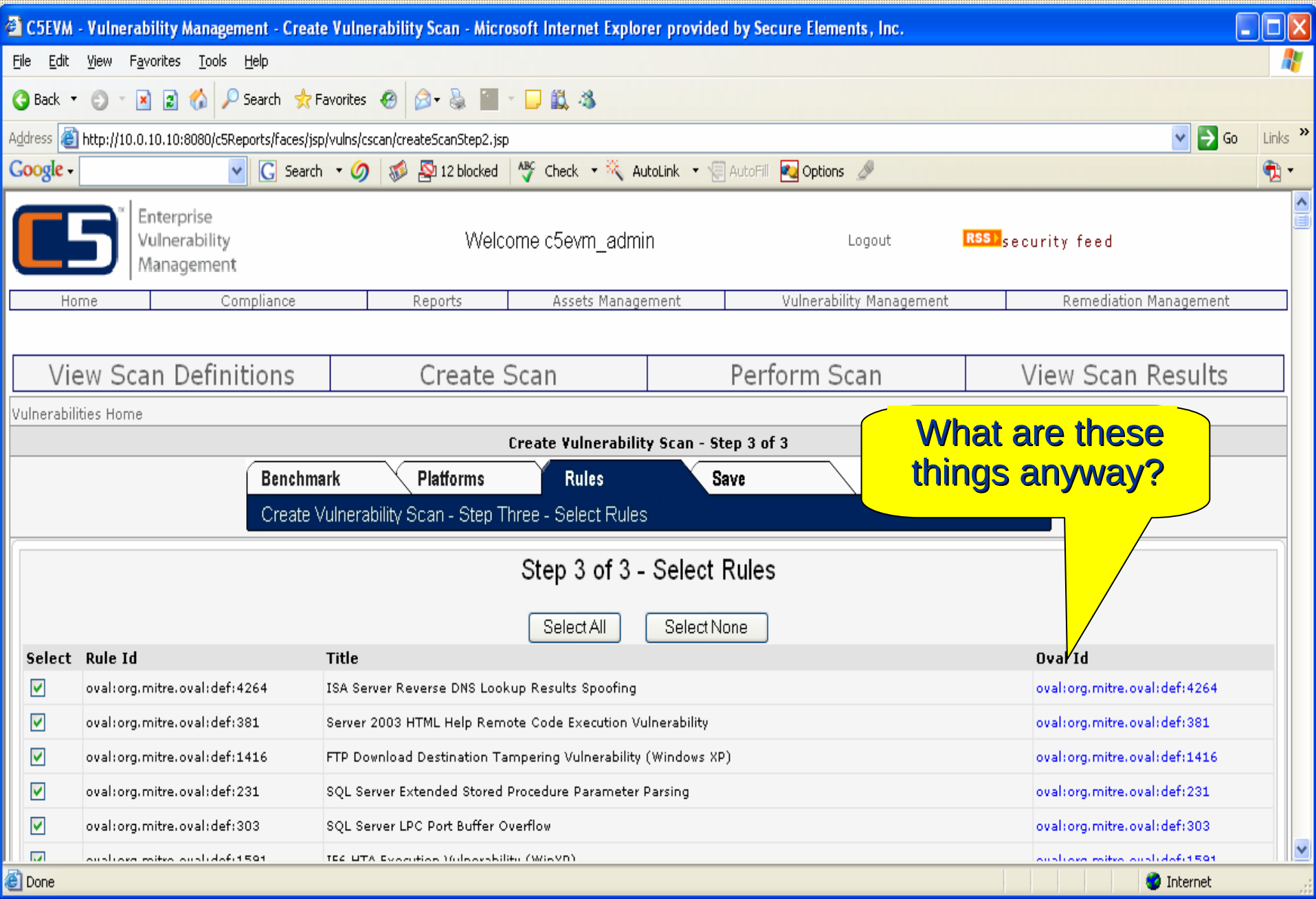
Vulnerability Scanning



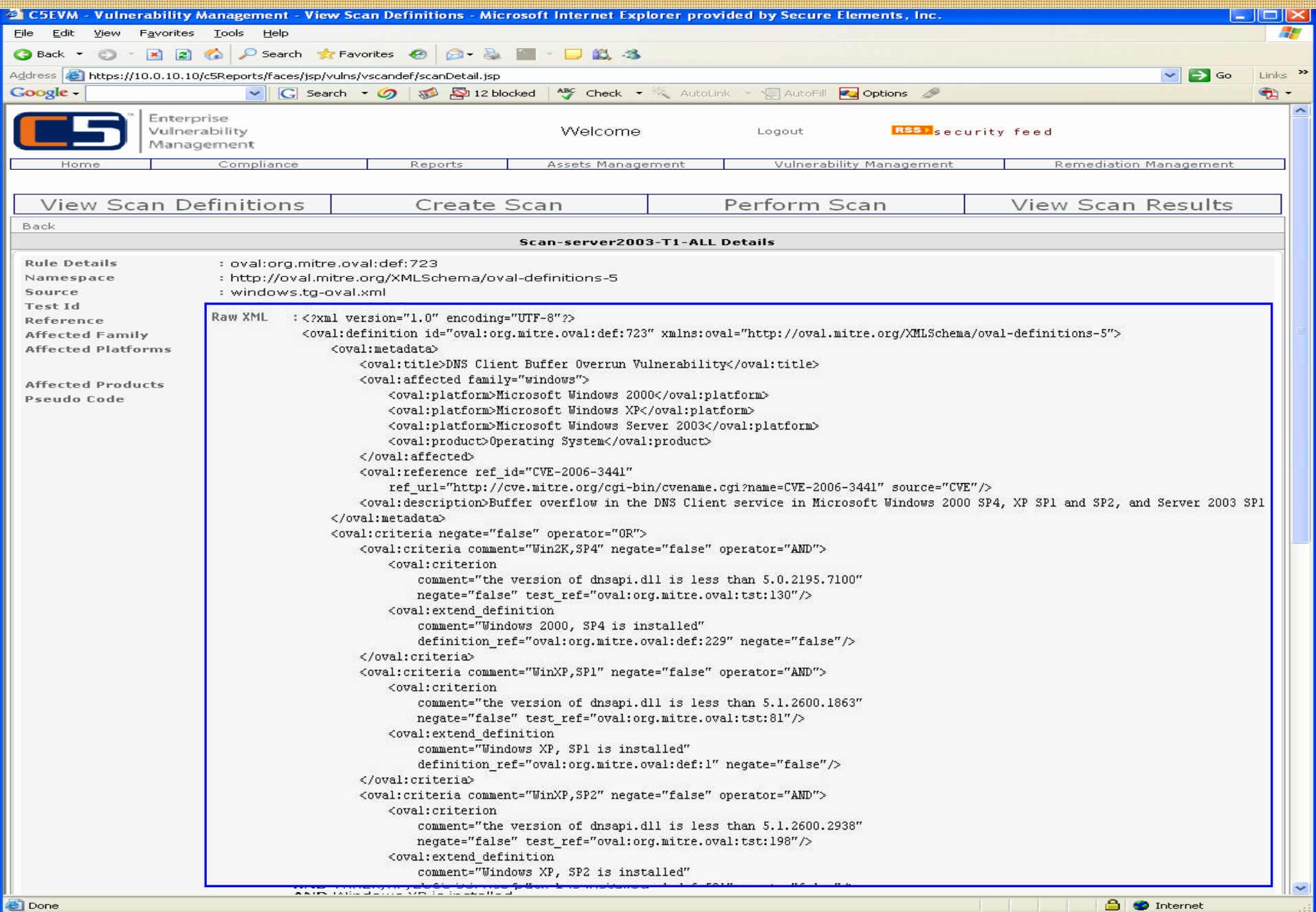
Vulnerability Scanning - Platforms



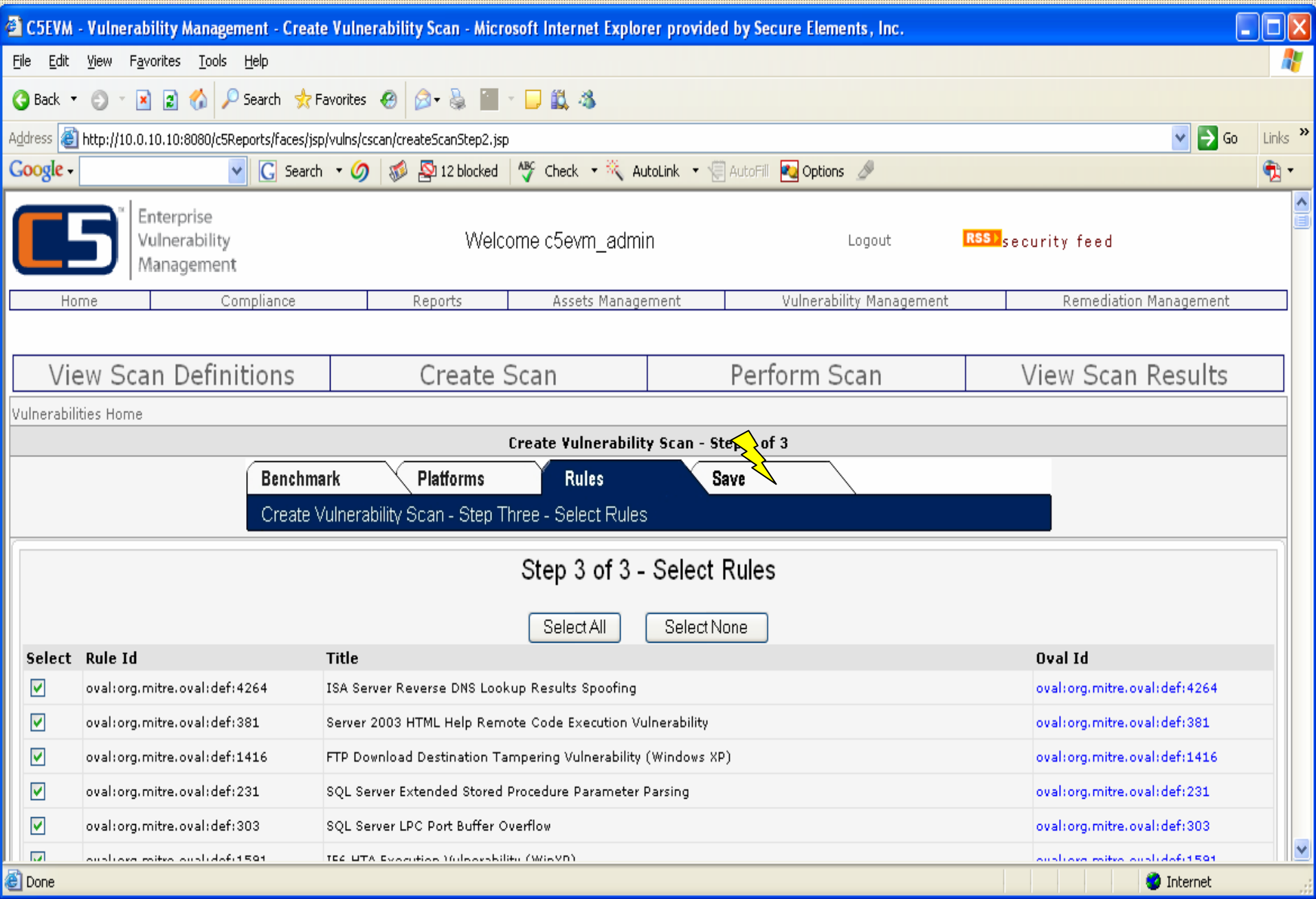
Vulnerability Scanning – Rule Selection



Rule Interrogation

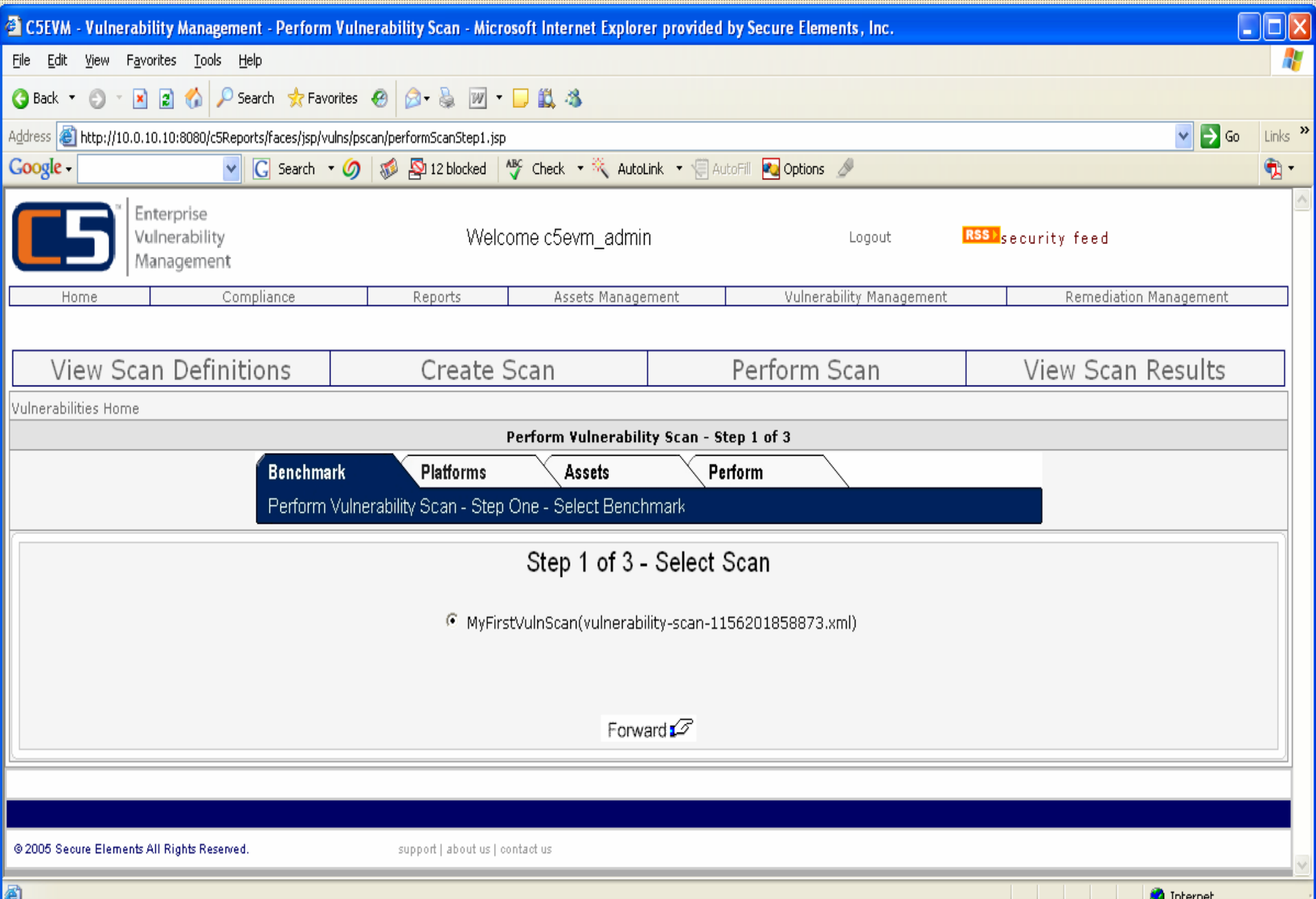


Vulnerability Scanning – Rule Selection

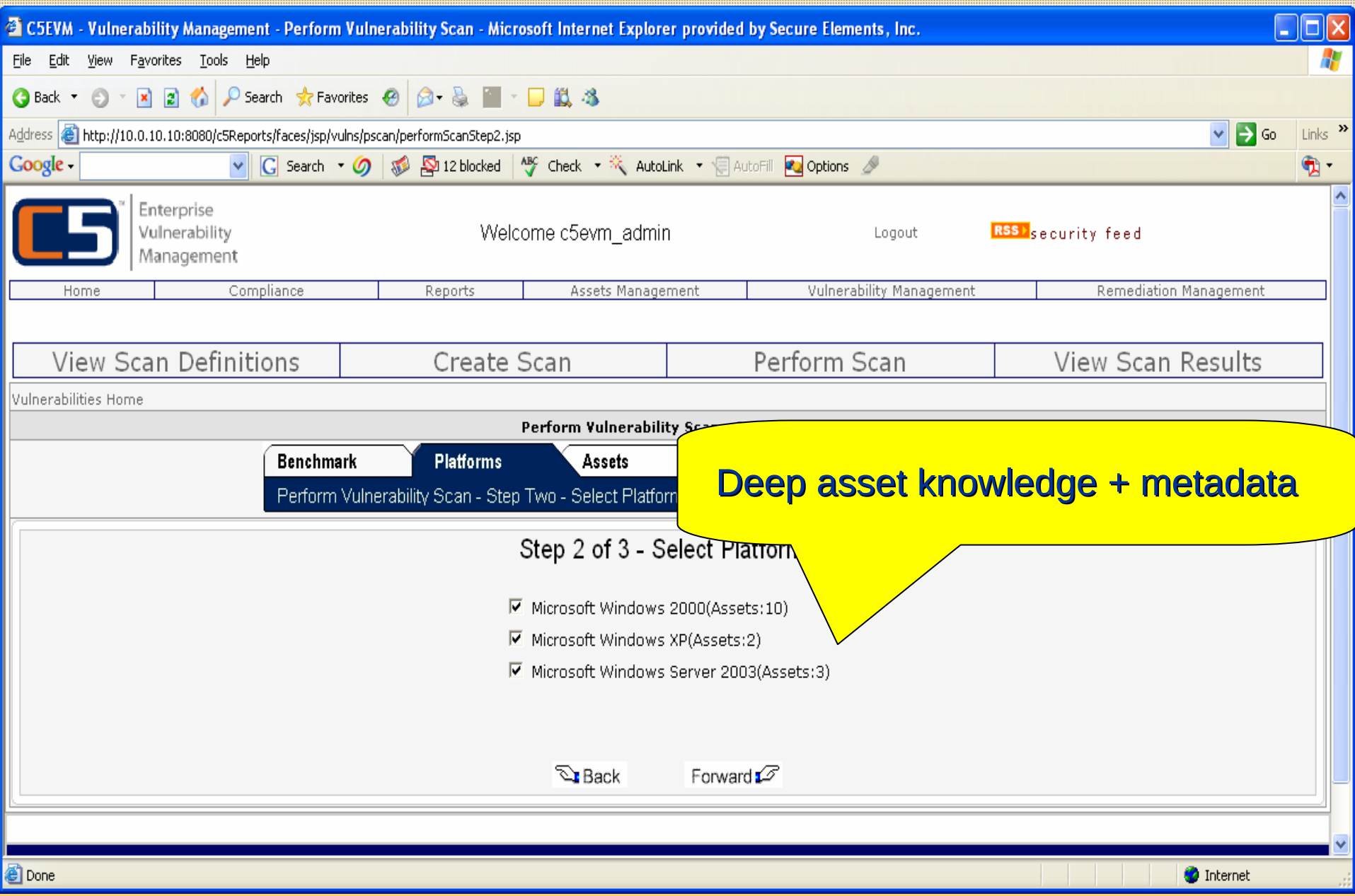


- Adapted Compliance Content
  - ✓ Various Sources
- Created A Vulnerability Scan

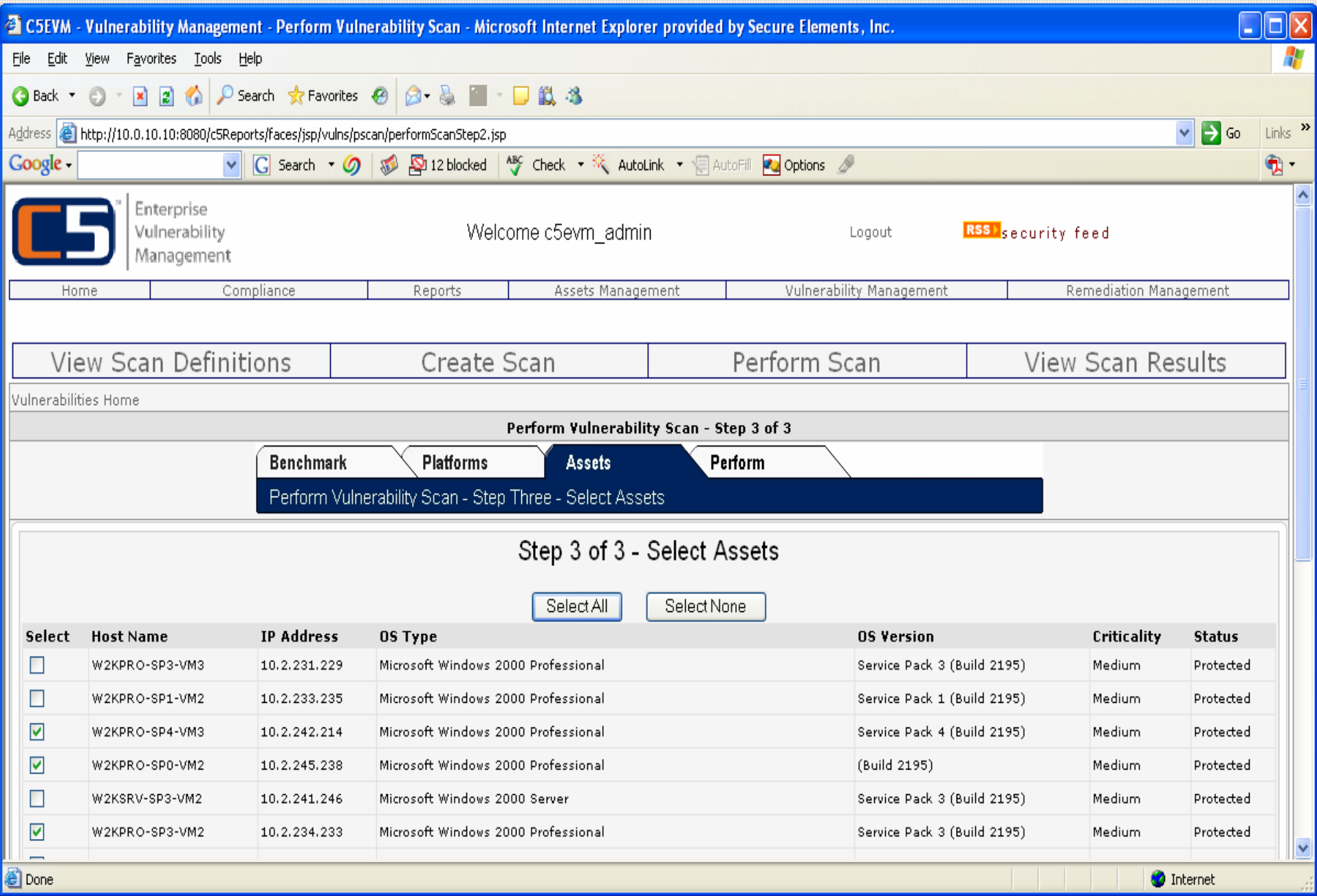
OVAL Scanning



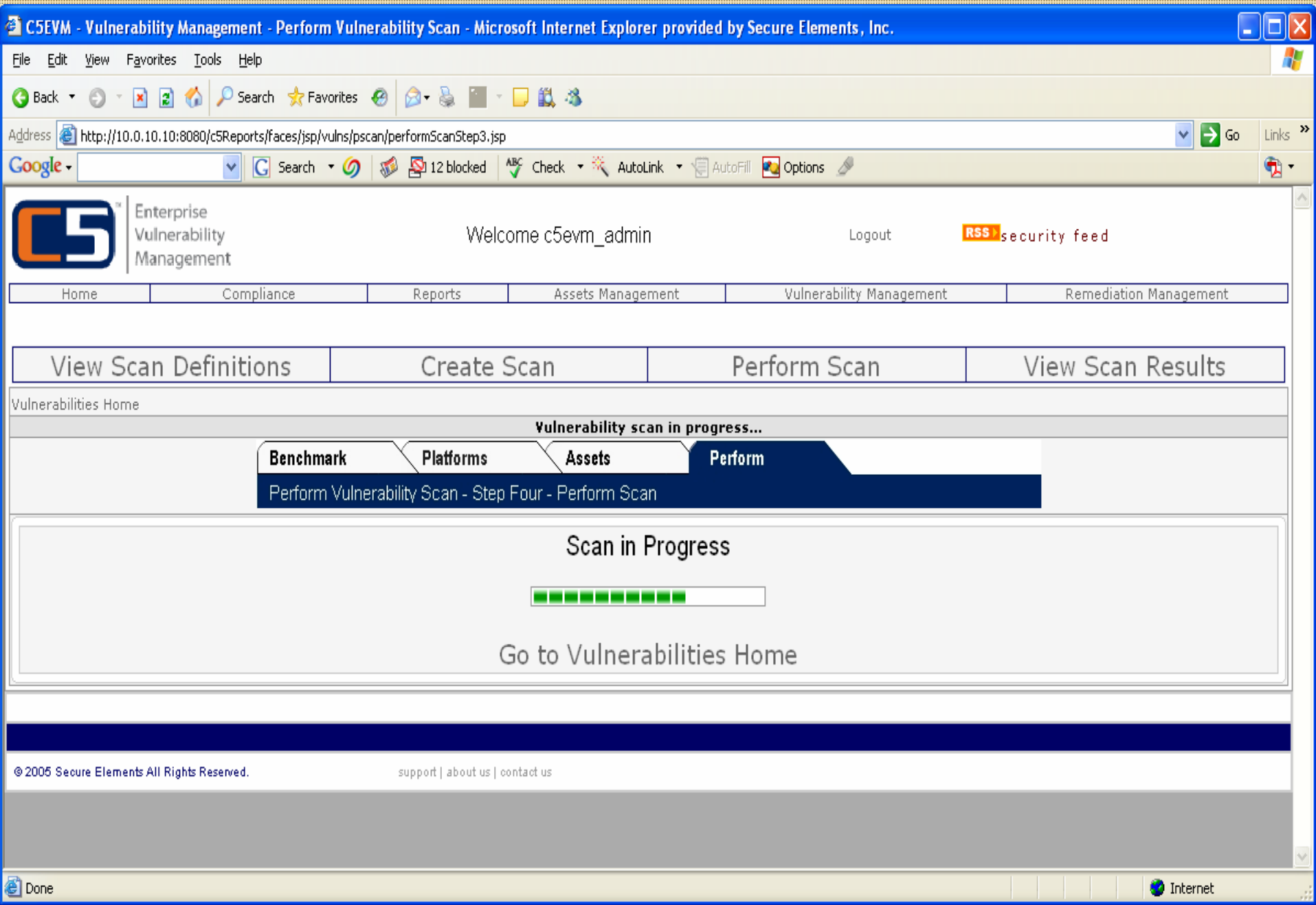
Apply an OVAL Vulnerability Scan



OVAL Scan Asset Selection



Perform OVAL Scan



C5EVM - Vulnerability Scan Results - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Search Favorites

Address http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/vscanres/scanTaskSummary.jsp Go Links

Google Search 12 blocked Check AutoLink AutoFill Options

Enterprise Vulnerability Management

Welcome c5evm_admin Logout RSS security feed

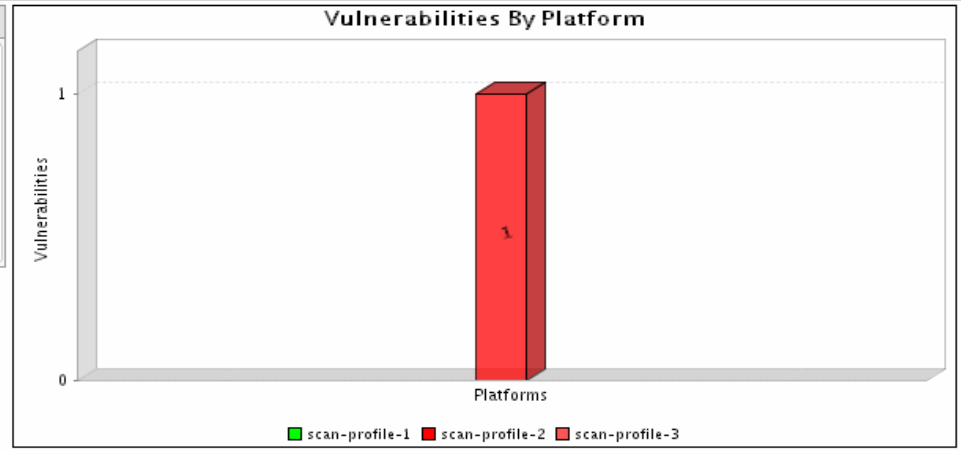
Home | Compliance | Reports | Assets Management | Vulnerability Management | Remediation Management

View Scan Definitions | Create Scan | Perform Scan | View Scan Results

Vulnerabilities Home → View Scan Results

Scan Summary

Property	Value
Name	vulnerability-scan-1156201858873.xml
Source	vulnerability-scan-1156201858873.xml
Applied By	c5evm_admin
Start Time	Mon, 21 Aug 2006 11:23:13 PM GMT
Status	In Progress
# of Assets	12
# of Vulnerabilities	1



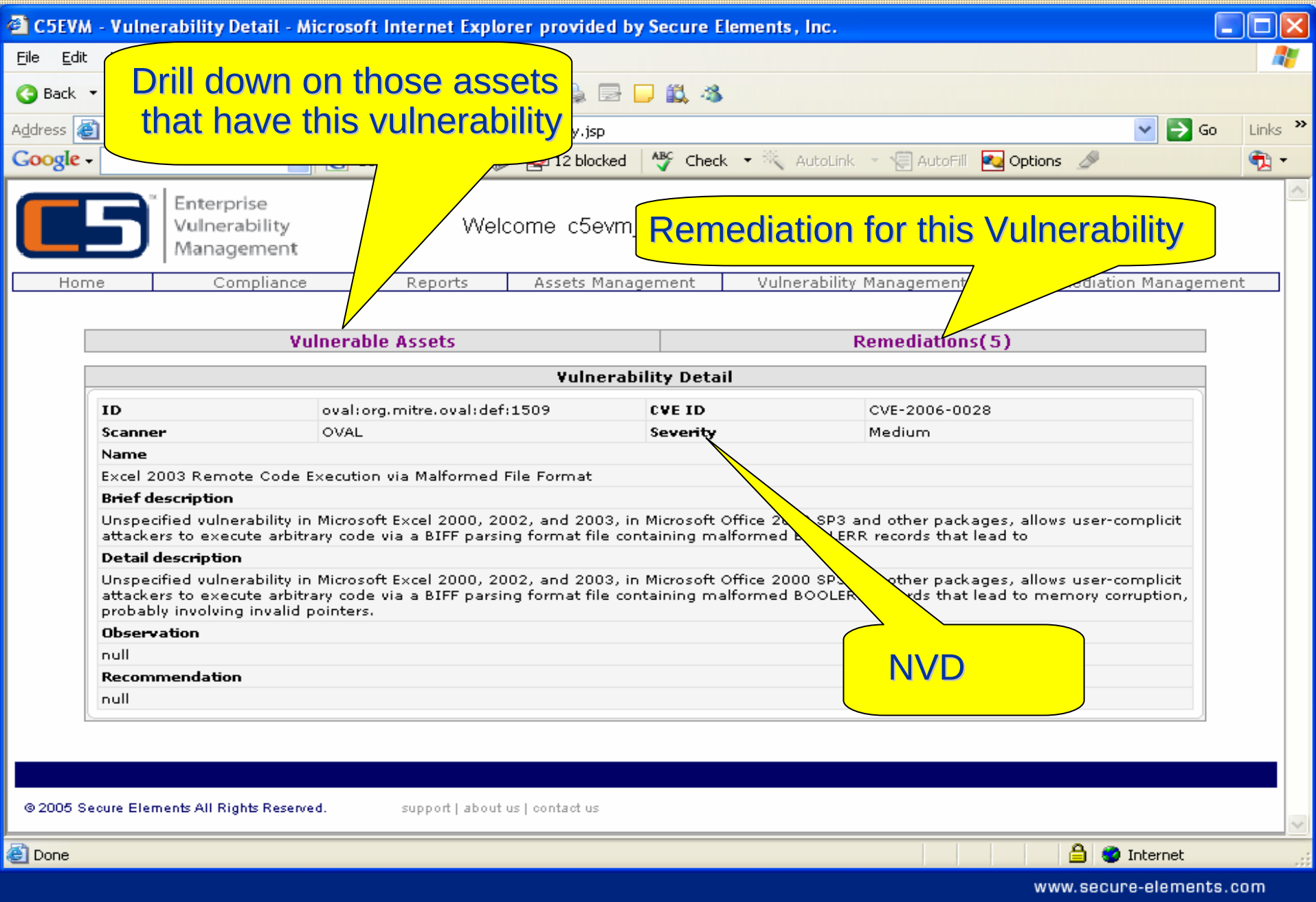
Compliance Assessment Evaluation - Benchmark Task Details

Platform	Start time	Completion Status	# of Assets	# of Vulnerabilities
scan-profile-1	Mon, 21 Aug 2006 11:23:25 PM GMT	0 %	7	0
scan-profile-2	Mon, 21 Aug 2006 11:23:21 PM GMT	100 %	3	1
scan-profile-3	Mon, 21 Aug 2006 11:23:13 PM GMT	0 %	2	0

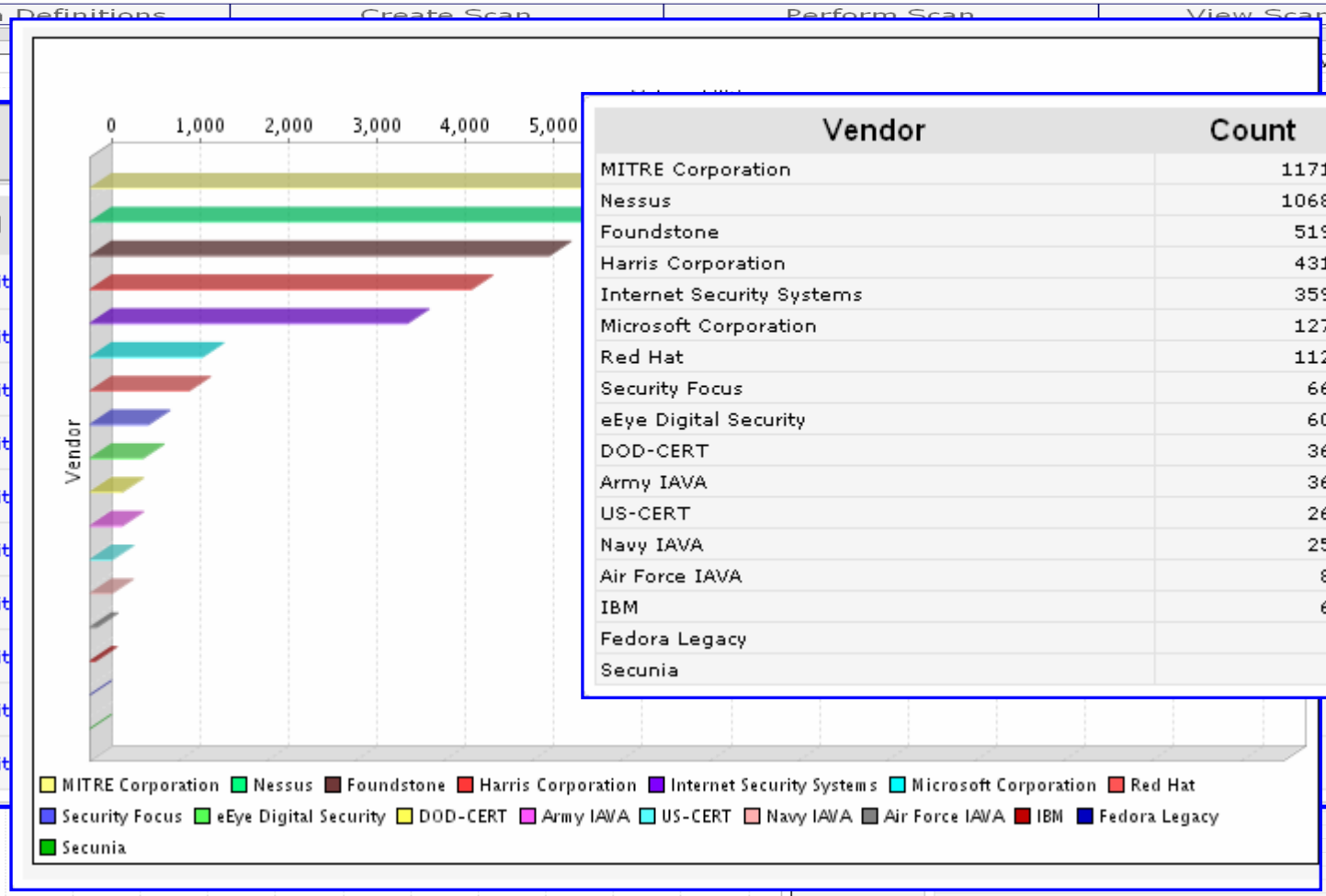
3 Records found, displaying 3 records, from 1 to 3. Page 1 / 1

Internet

Vulnerability Detail

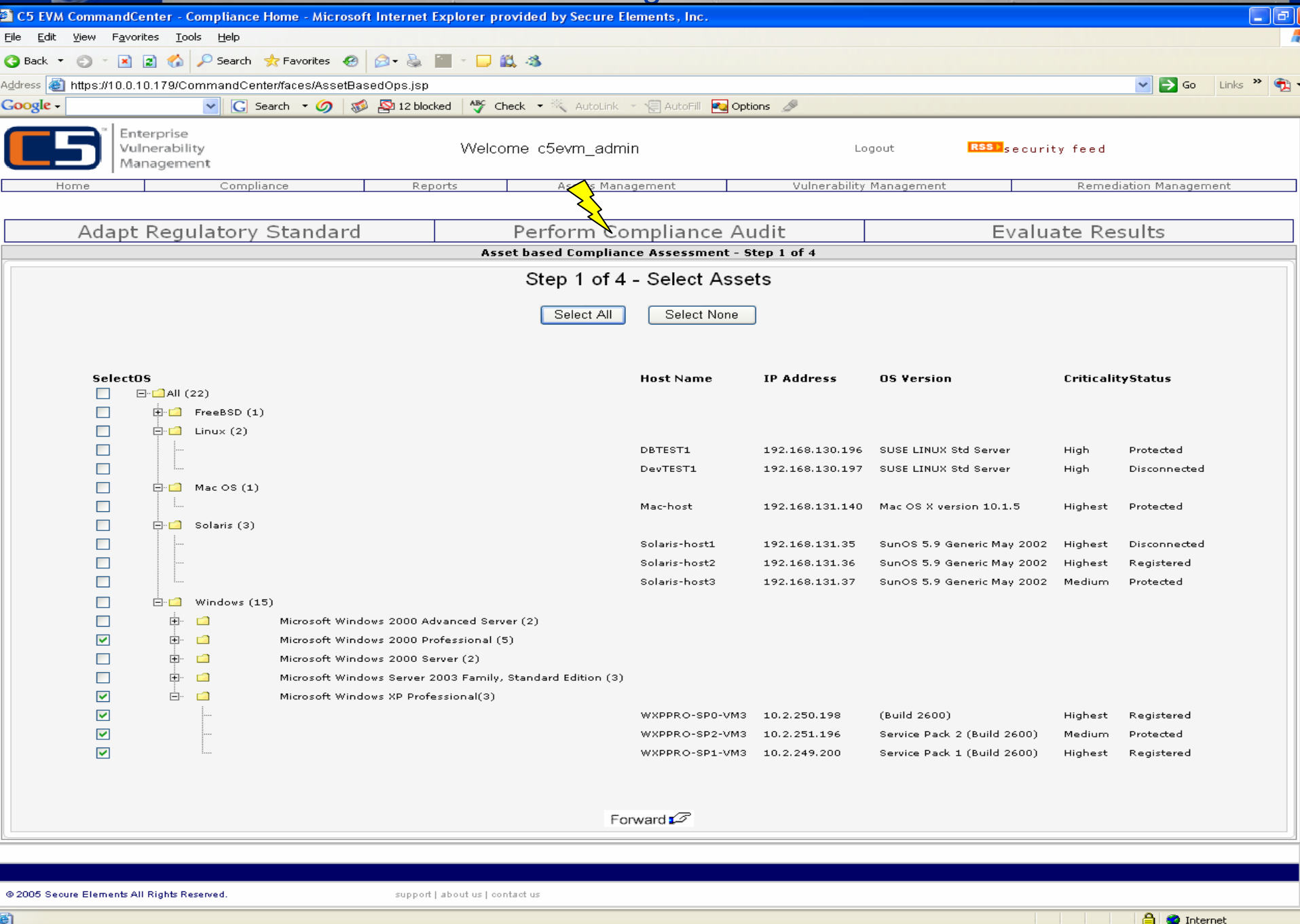


Enterprise Vulnerability View

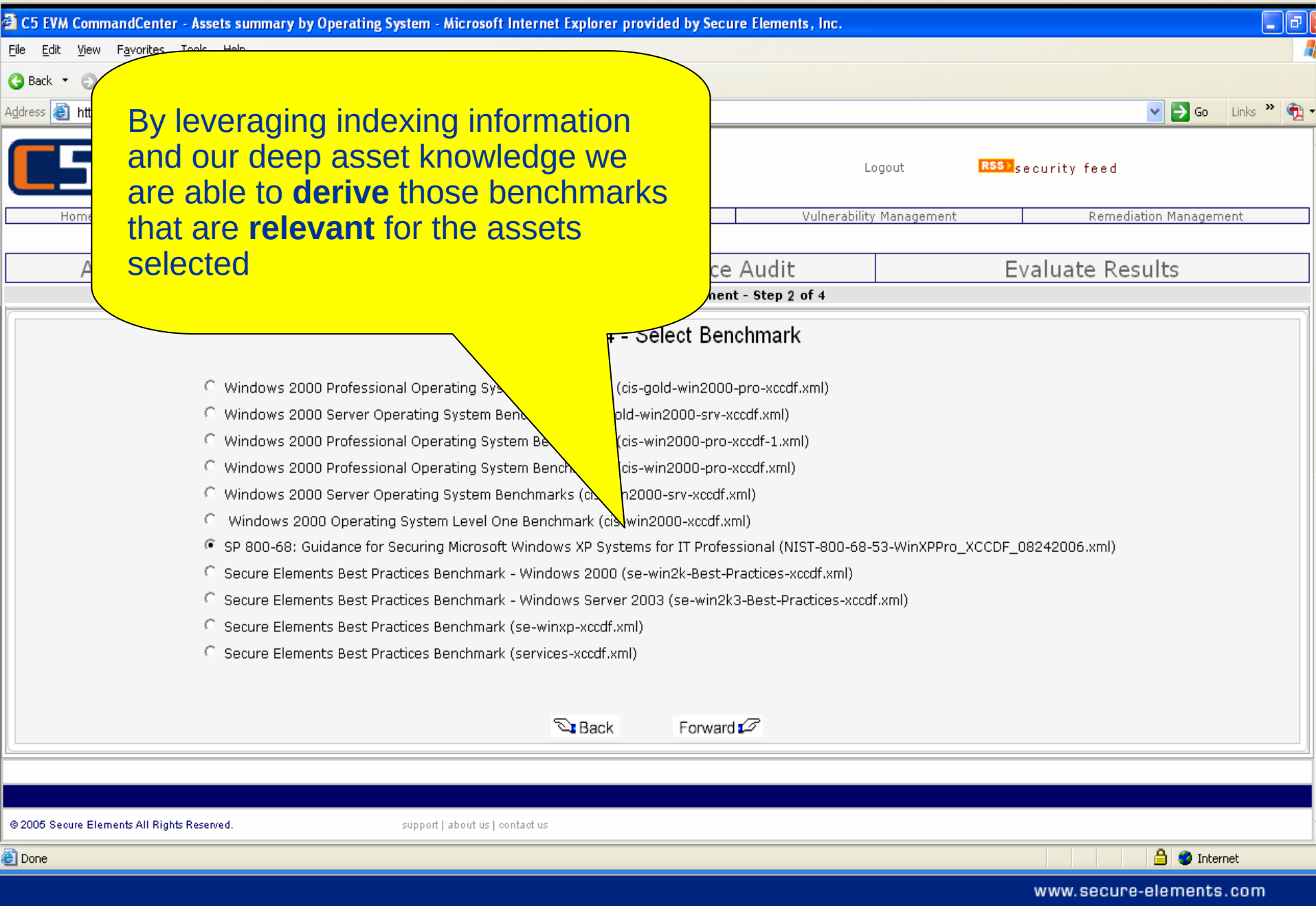


Vendor	Count
MITRE Corporation	11718
Nessus	10680
Foundstone	5195
Harris Corporation	4314
Internet Security Systems	3595
Microsoft Corporation	1278
Red Hat	1127
Security Focus	668
eEye Digital Security	602
DOD-CERT	368
Army IAVA	368
US-CERT	260
Navy IAVA	255
Air Force IAVA	83
IBM	69
Fedora Legacy	6
Secunia	4

Performing the Audit

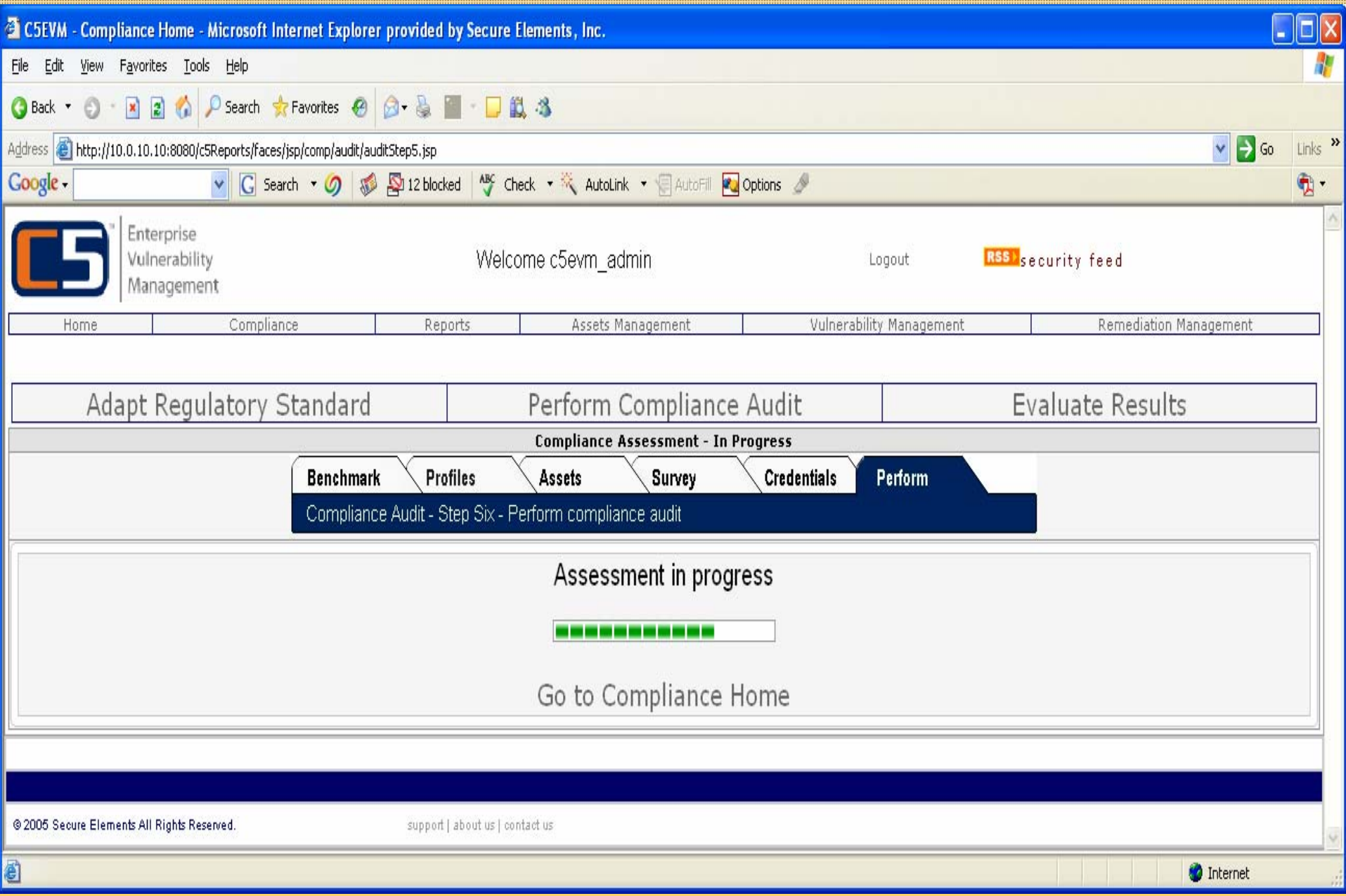


Dynamic Derivation of Applicable Benchmarks

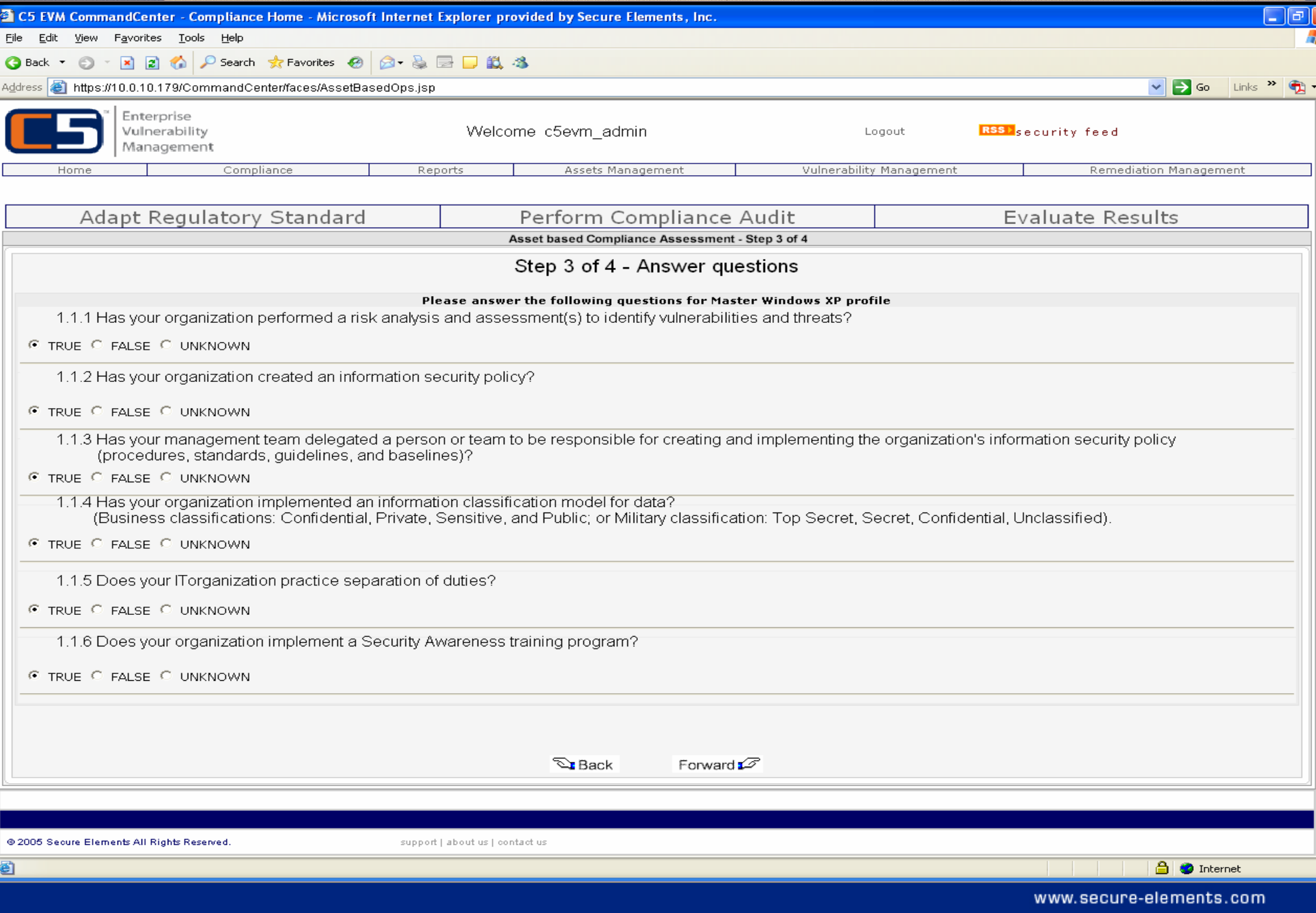


By leveraging indexing information and our deep asset knowledge we are able to **derive** those benchmarks that are **relevant** for the assets selected

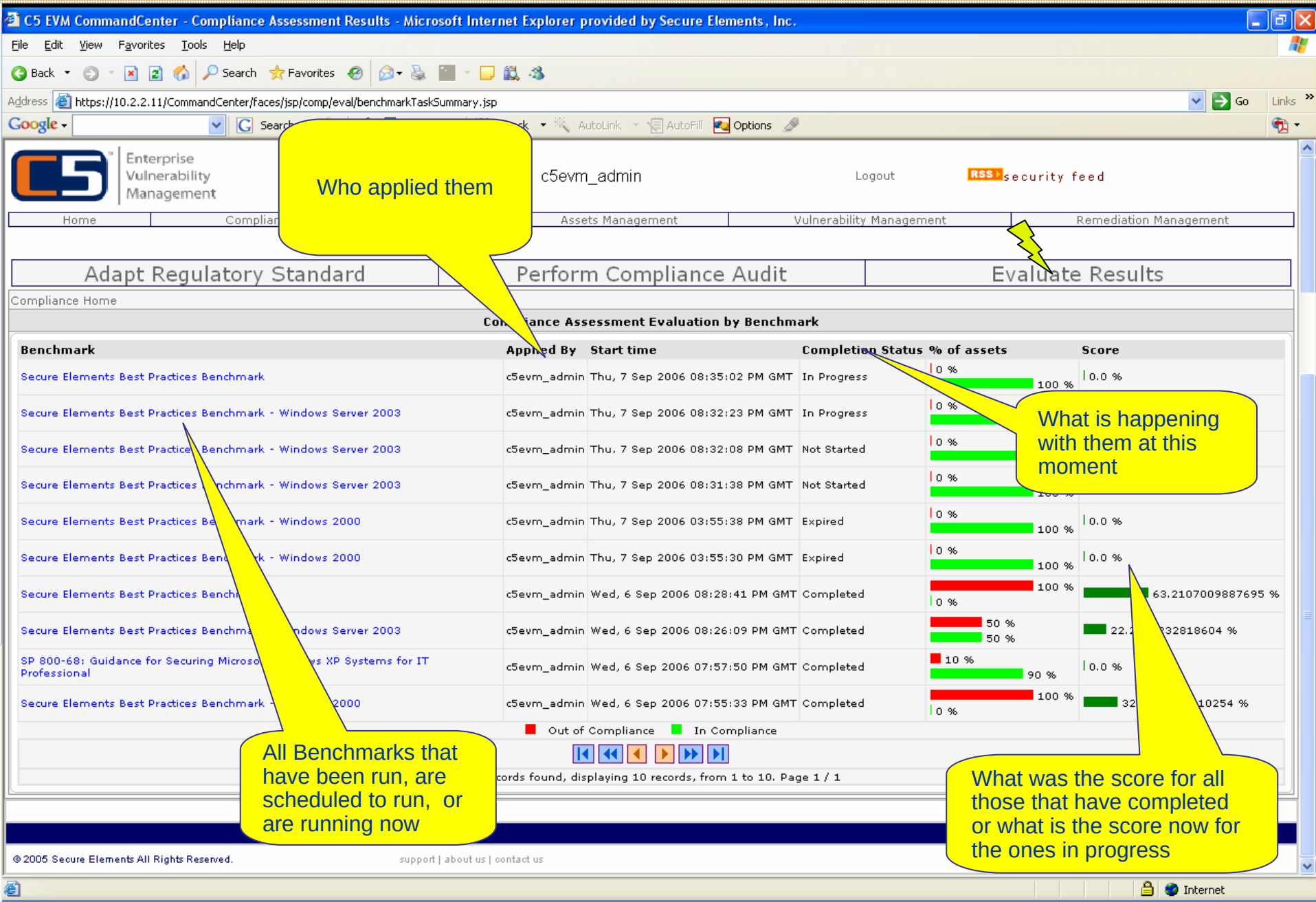
Perform the Audit



Non-Technical Controls



Compliance Home



Who applied them

What is happening with them at this moment

All Benchmarks that have been run, are scheduled to run, or are running now

What was the score for all those that have completed or what is the score now for the ones in progress

Compliance Benchmark Summary

C5 EVM CommandCenter - Compliance Assessment Results - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Search Favorites

Address https://10.2.2.11/CommandCenter/faces/jsp/comp/eval/benchmarkTaskSummary.jsp Go Links

Google Search 12 blocked Check AutoLink AutoFill Options

C5 Enterprise Vulnerability Management

Welcome c5evm_admin Logout RSS security feed

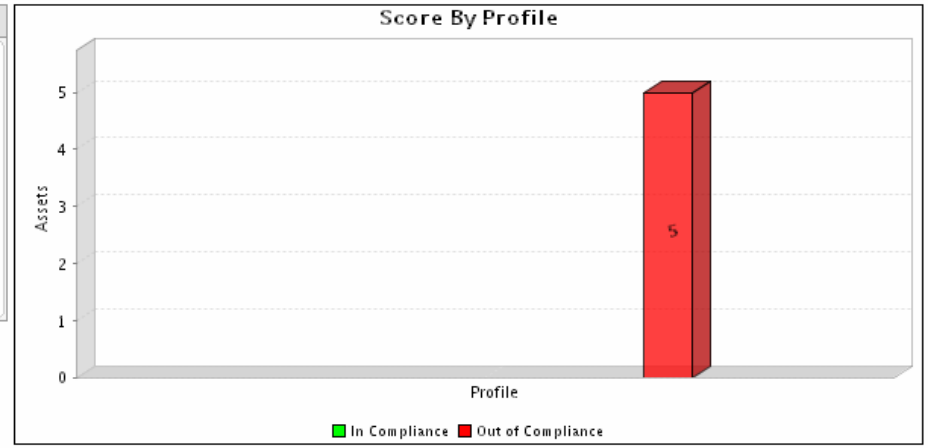
Home | Compliance | Reports | Assets Management | Vulnerability Management | Remediation Management

Adapt Regulatory Standard | Perform Compliance Audit | Evaluate Results

Compliance Home → Evaluate Home

Benchmark Summary

Property	Value
Name	Windows 2000 Professional Operating System Benchmarks
Source	cis-gold-win2000-pro-xccdf.xml
Applied By	c5evm_admin
Start Time	Tue, 12 Sep 2006 11:18:43 PM GMT
Status	Completed
# of Assets	5
Out of Compliance	100 % assets
In Compliance	0 % assets
Score	58.3333320617676 %



Compliance Assessment Evaluation - Benchmark Task Details

Profile	Start time	Completion Status	Total Assets	Result	Score
Level II	Tue, 12 Sep 2006 11:18:43 PM GMT	100 %	5	100 % 0 %	58.3333320617676 %

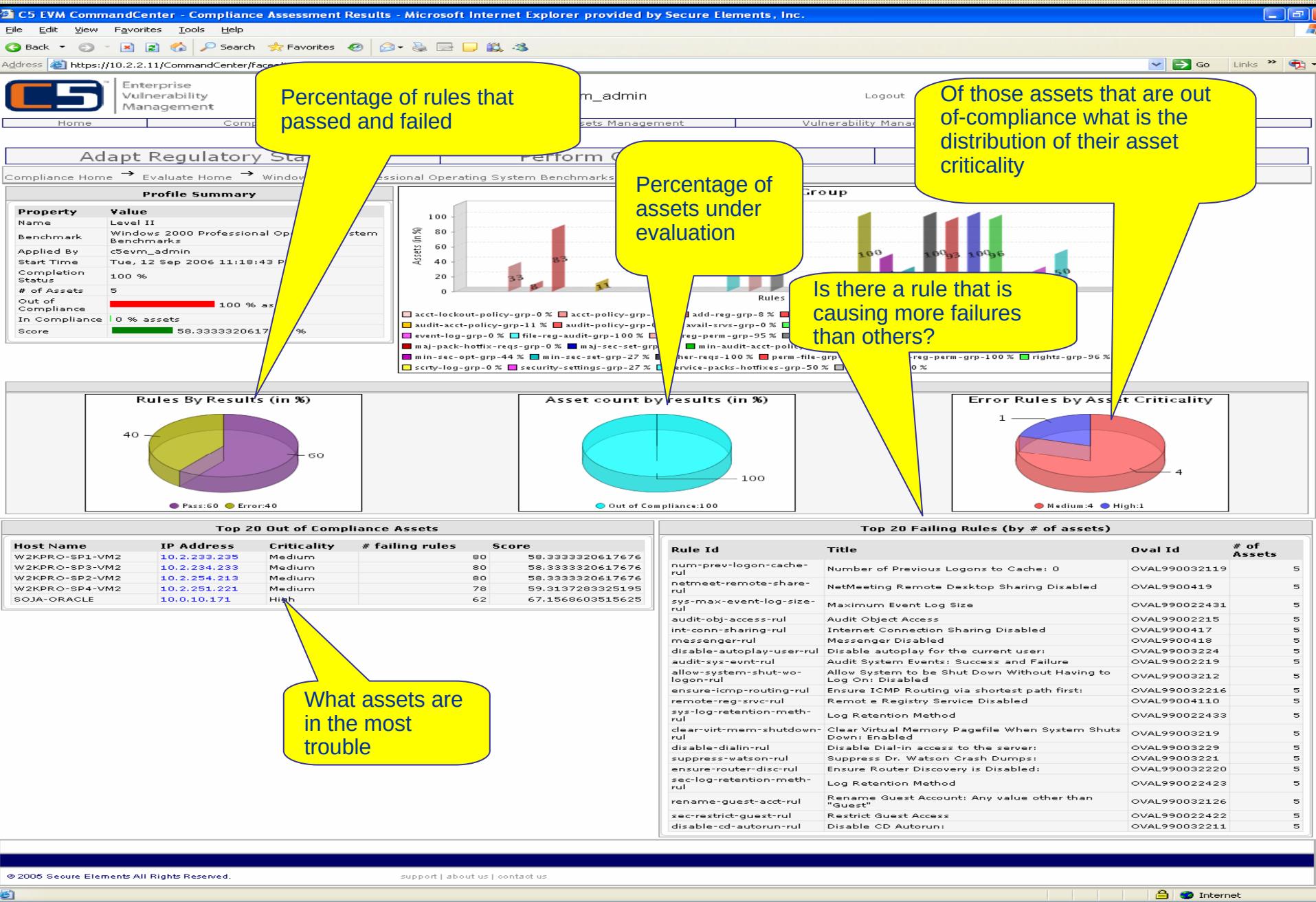
Out of Compliance In Compliance

1 Records found, displaying 1 records, from 1 to 1. Page 1 / 1

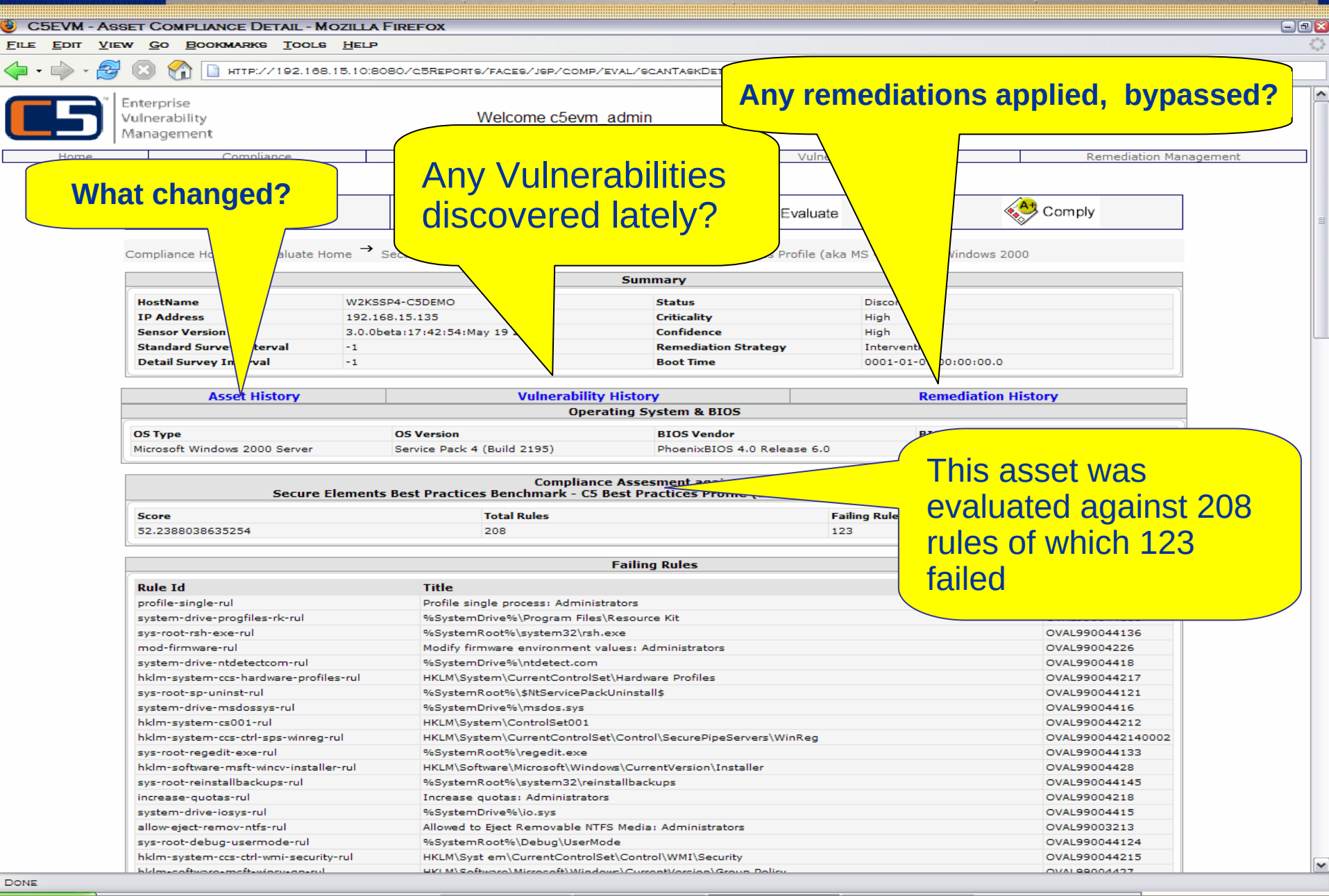
support | about us | contact us

Done Internet

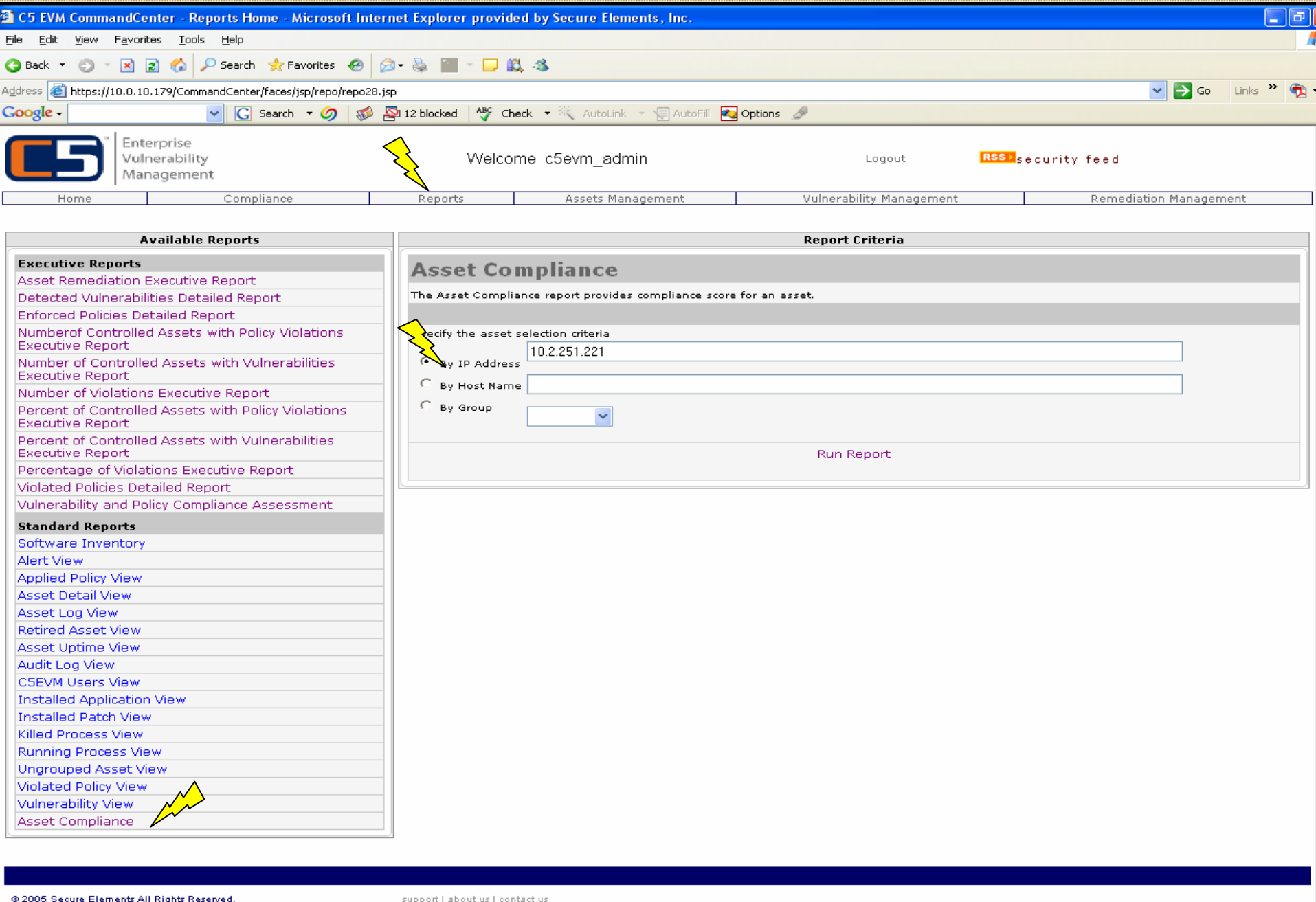
Compliance Profile Summary



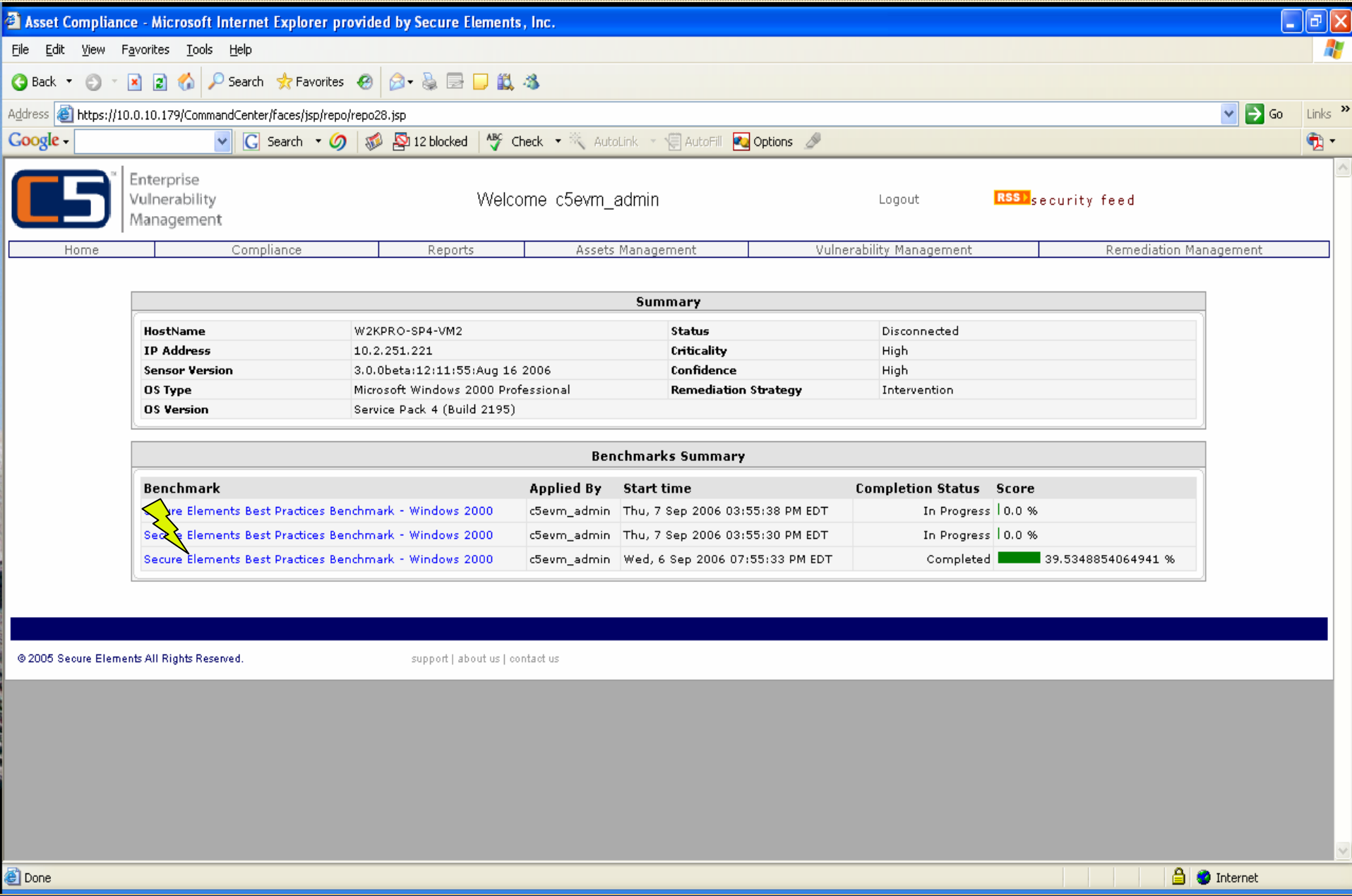
Compliance


C5EVM - Asset Compliance Detail - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Enterprise Vulnerability Management
Welcome c5evm_admin
Home
Compliance
Remediation Management
Evaluate
Comply
What changed?
Any Vulnerabilities discovered lately?
Any remediations applied, bypassed?
Summary
HostName W2KSSP4-C5DEMO
IP Address 192.168.15.135
Sensor Version 3.0.0beta:17:42:54:May 19
Standard Survey Interval -1
Detail Survey Interval -1
Status
Criticality High
Confidence High
Remediation Strategy
Boot Time
Asset History
Vulnerability History
Remediation History
Operating System & BIOS
OS Type
Microsoft Windows 2000 Server
OS Version
Service Pack 4 (Build 2195)
BIOS Vendor
PhoenixBIOS 4.0 Release 6.0
Secure Elements Best Practices Benchmark - C5 Best Practices
Score
52.2388038635254
Total Rules
208
Failing Rules
123
This asset was evaluated against 208 rules of which 123 failed
Failing Rules
Rule Id
Title
profile-single-rul
Profile single process: Administrators
system-drive-progfiles-rk-rul
%SystemDrive%\Program Files\Resource Kit
sys-root-rsh-exe-rul
%SystemRoot%\system32\rsh.exe
OVAL990044136
mod-firmware-rul
Modify firmware environment values: Administrators
OVAL99004226
system-drive-ntdetectcom-rul
%SystemDrive%\ntdetect.com
OVAL99004418
hklm-system-ccs-hardware-profiles-rul
HKLM\System\CurrentControlSet\Hardware Profiles
OVAL990044217
sys-root-sp-uninst-rul
%SystemRoot%\$NtServicePackUninstall$
OVAL990044121
system-drive-msdossys-rul
%SystemDrive%\msdos.sys
OVAL99004416
hklm-system-cs001-rul
HKLM\System\ControlSet001
OVAL990044212
hklm-system-ccs-ctrl-sps-winreg-rul
HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg
OVAL9900442140002
sys-root-regedit-exe-rul
%SystemRoot%\regedit.exe
OVAL990044133
hklm-software-msft-wincv-installer-rul
HKLM\Software\Microsoft\Windows\CurrentVersion\Installer
OVAL99004428
sys-root-reinstallbackups-rul
%SystemRoot%\system32\reinstallbackups
OVAL990044145
increase-quotas-rul
Increase quotas: Administrators
OVAL99004218
system-drive-iosys-rul
%SystemDrive%\io.sys
OVAL99004415
allow-eject-remov-ntfs-rul
Allowed to Eject Removable NTFS Media: Administrators
OVAL99003213
sys-root-debug-usermode-rul
%SystemRoot%\Debug\UserMode
OVAL990044124
hklm-system-ccs-ctrl-wmi-security-rul
HKLM\Syst em\CurrentControlSet\Control\WMI\Security
OVAL990044215
Done

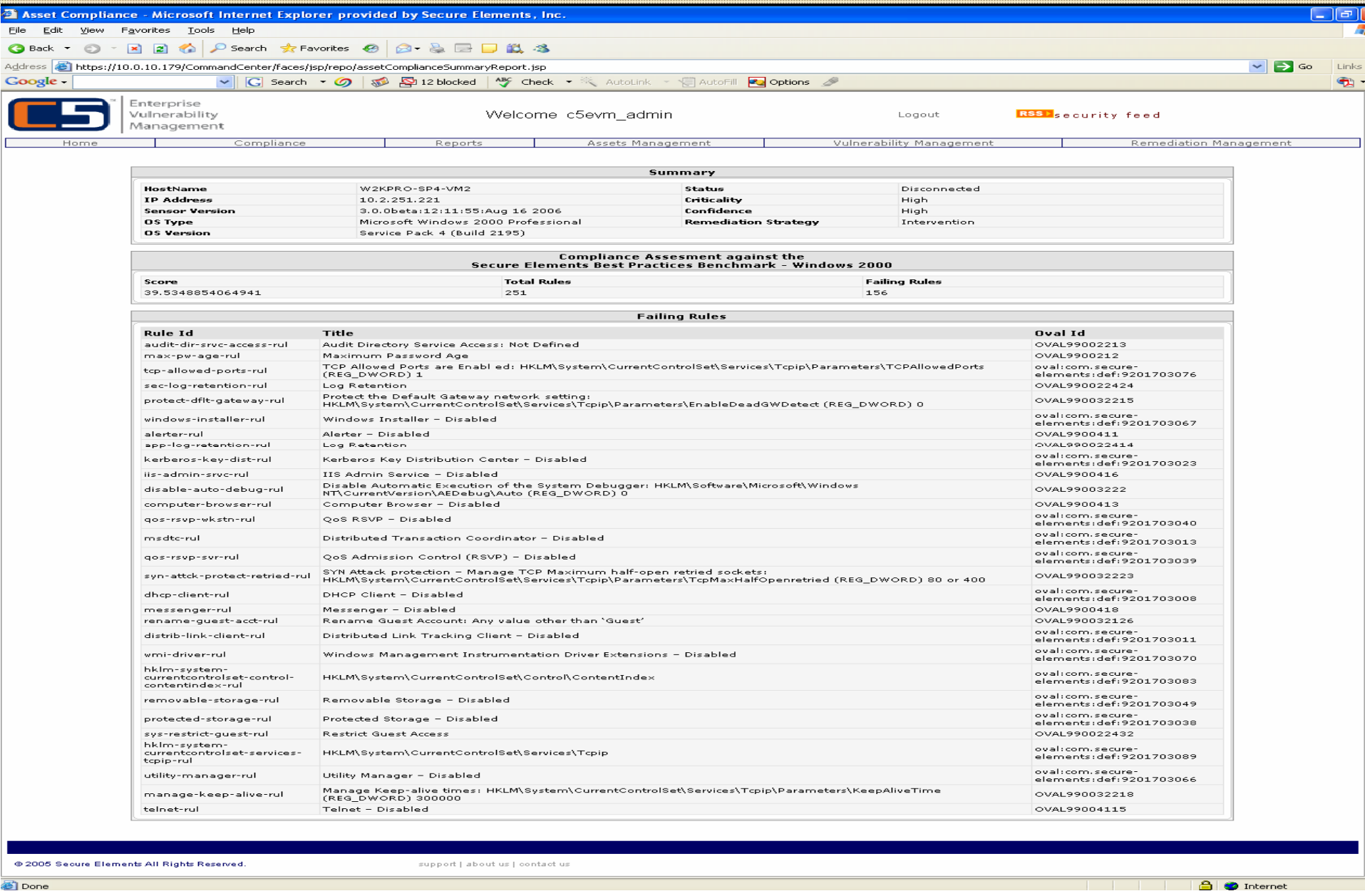
Compliance Report Generation



Active HTML View



Detailed Asset Compliance Report



Asset Compliance - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Search Favorites

Address https://10.0.10.179/CommandCenter/Faces/jsp/repo/assetComplianceSummaryReport.jsp

Google Search 12 blocked Check AutoLink AutoFill Options

Enterprise Vulnerability Management

Welcome c5evm_admin Logout RSS security feed

Home | Compliance | Reports | Assets Management | Vulnerability Management | Remediation Management

Summary

HostName	W2KPRO-SP4-VM2	**Status**	Disconnected
IP Address	10.2.251.221	**Criticality**	High
Sensor Version	3.0.0beta:12:11:55:Aug 16 2006	**Confidence**	High
OS Type	Microsoft Windows 2000 Professional	**Remediation Strategy**	Intervention
OS Version	Service Pack 4 (Build 2195)		

Compliance Assesment against the Secure Elements Best Practices Benchmark - Windows 2000

Score	Total Rules	Failing Rules
39.5348854064941	251	156

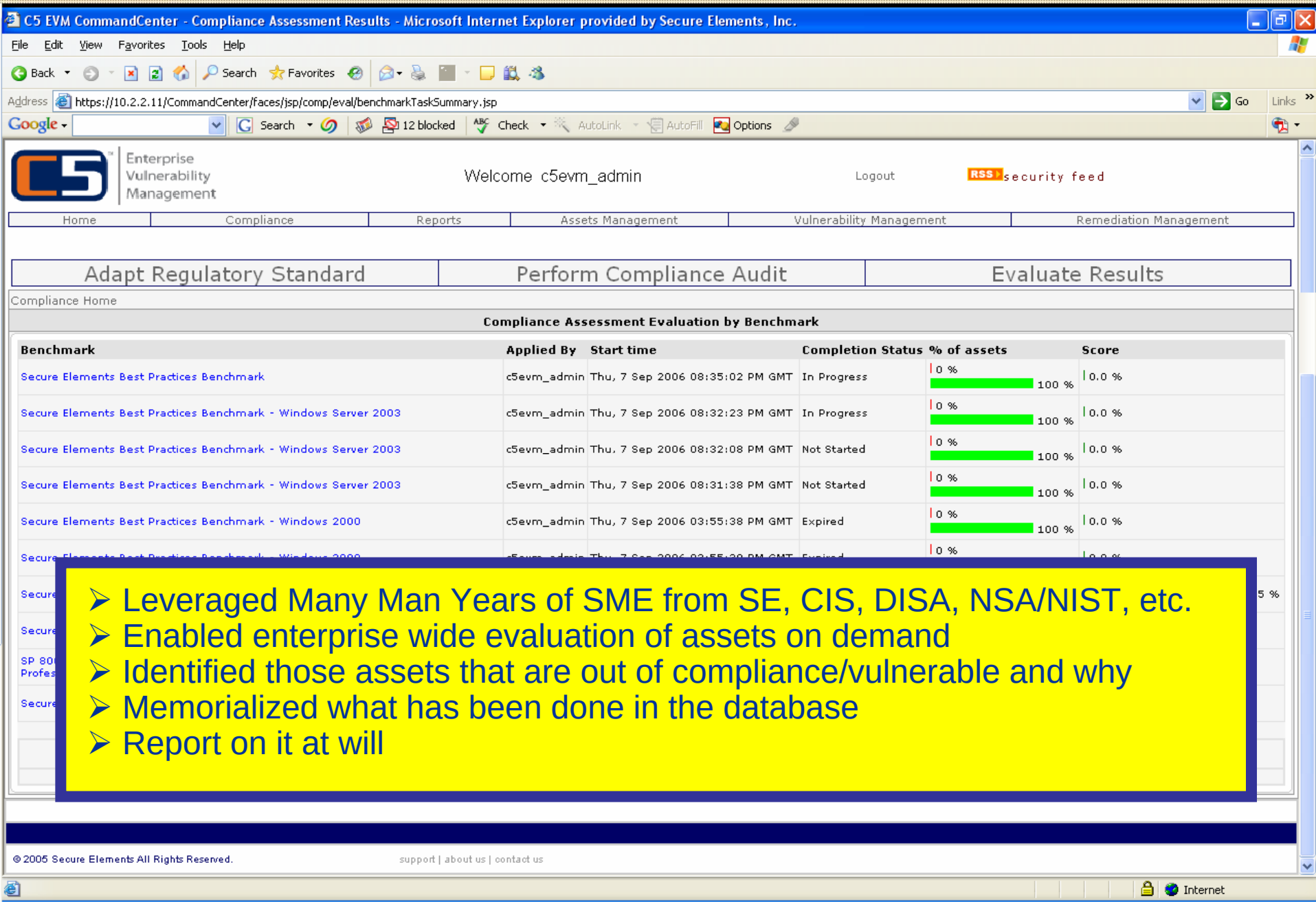
Failing Rules

Rule Id	Title	Oval Id
audit-dir-srvc-access-rul	Audit Directory Service Access: Not Defined	OVAL99002213
max-pw-age-rul	Maximum Password Age	OVAL9900212
tcp-allowed-ports-rul	TCP Allowed Ports are Enabl ed: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPAllowedPorts (REG_DWORD) 1	oval:com.secure-elements:def:9201703076
sec-log-retention-rul	Log Retention	OVAL990022424
protect-dflt-gateway-rul	Protect the Default Gateway network setting: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect (REG_DWORD) 0	OVAL990032215
windows-installer-rul	Windows Installer – Disabled	oval:com.secure-elements:def:9201703067
alerter-rul	Alerter – Disabled	OVAL9900411
app-log-retention-rul	Log Retention	OVAL990022414
kerberos-key-dist-rul	Kerberos Key Distribution Center – Disabled	oval:com.secure-elements:def:9201703023
iis-admin-srvc-rul	IIS Admin Service – Disabled	OVAL9900416
disable-auto-debug-rul	Disable Automatic Execution of the System Debugger: HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto (REG_DWORD) 0	OVAL99003222
computer-browser-rul	Computer Browser – Disabled	OVAL9900413
qos-rsvp-wkstn-rul	QoS RSVP – Disabled	oval:com.secure-elements:def:9201703040
msdtc-rul	Distributed Transaction Coordinator – Disabled	oval:com.secure-elements:def:9201703013
qos-rsvp-svr-rul	QoS Admission Control (RSVP) – Disabled	oval:com.secure-elements:def:9201703039
syn-attck-protect-retried-rul	SYN Attack protection – Manage TCP Maximum half-open retried sockets: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenretried (REG_DWORD) 80 or 400	OVAL990032223
dhcp-client-rul	DHCP Client – Disabled	oval:com.secure-elements:def:9201703008
messenger-rul	Messenger – Disabled	OVAL9900418
rename-guest-acct-rul	Rename Guest Account: Any value other than 'Guest'	OVAL990032126
distrib-link-client-rul	Distributed Link Tracking Client – Disabled	oval:com.secure-elements:def:9201703011
wmi-driver-rul	Windows Management Instrumentation Driver Extensions – Disabled	oval:com.secure-elements:def:9201703070
hklm-system-currentcontrolset-control-contentindex-rul	HKLM\System\CurrentControlSet\Control\ContentIndex	oval:com.secure-elements:def:9201703083
removable-storage-rul	Removable Storage – Disabled	oval:com.secure-elements:def:9201703049
protected-storage-rul	Protected Storage – Disabled	oval:com.secure-elements:def:9201703038
sys-restrict-guest-rul	Restrict Guest Access	OVAL990022432
hklm-system-currentcontrolset-services-tcpip-rul	HKLM\System\CurrentControlSet\Services\Tcpip	oval:com.secure-elements:def:9201703089
utility-manager-rul	Utility Manager – Disabled	oval:com.secure-elements:def:9201703066
manage-keep-alive-rul	Manage Keep-alive times: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime (REG_DWORD) 300000	OVAL990032218
telnet-rul	Telnet – Disabled	OVAL99004115

support | about us | contact us

Done Internet

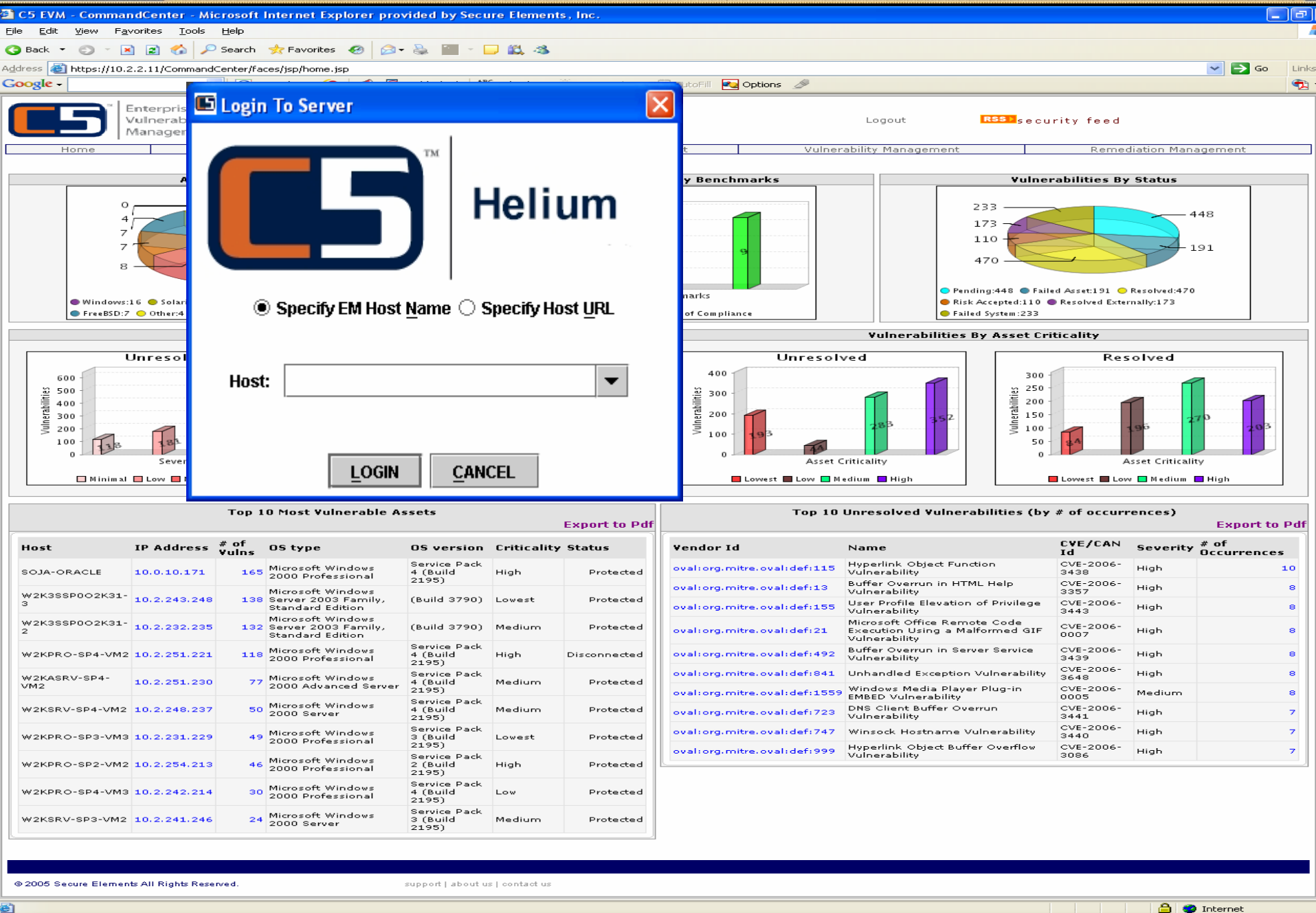
Enterprise Compliance



- Leveraged Many Man Years of SME from SE, CIS, DISA, NSA/NIST, etc.
- Enabled enterprise wide evaluation of assets on demand
- Identified those assets that are out of compliance/vulnerable and why
- Memorialized what has been done in the database
- Report on it at will

- Pareto's principle
  - "for many phenomena 80% of consequences stem from 20% of the causes."
- 80% Use cases can be addressed by the abstraction
- 20% Require getting out of the abstraction

C5 Helium Content “Browser”



Top 10 Most Vulnerable Assets

Export to Pdf

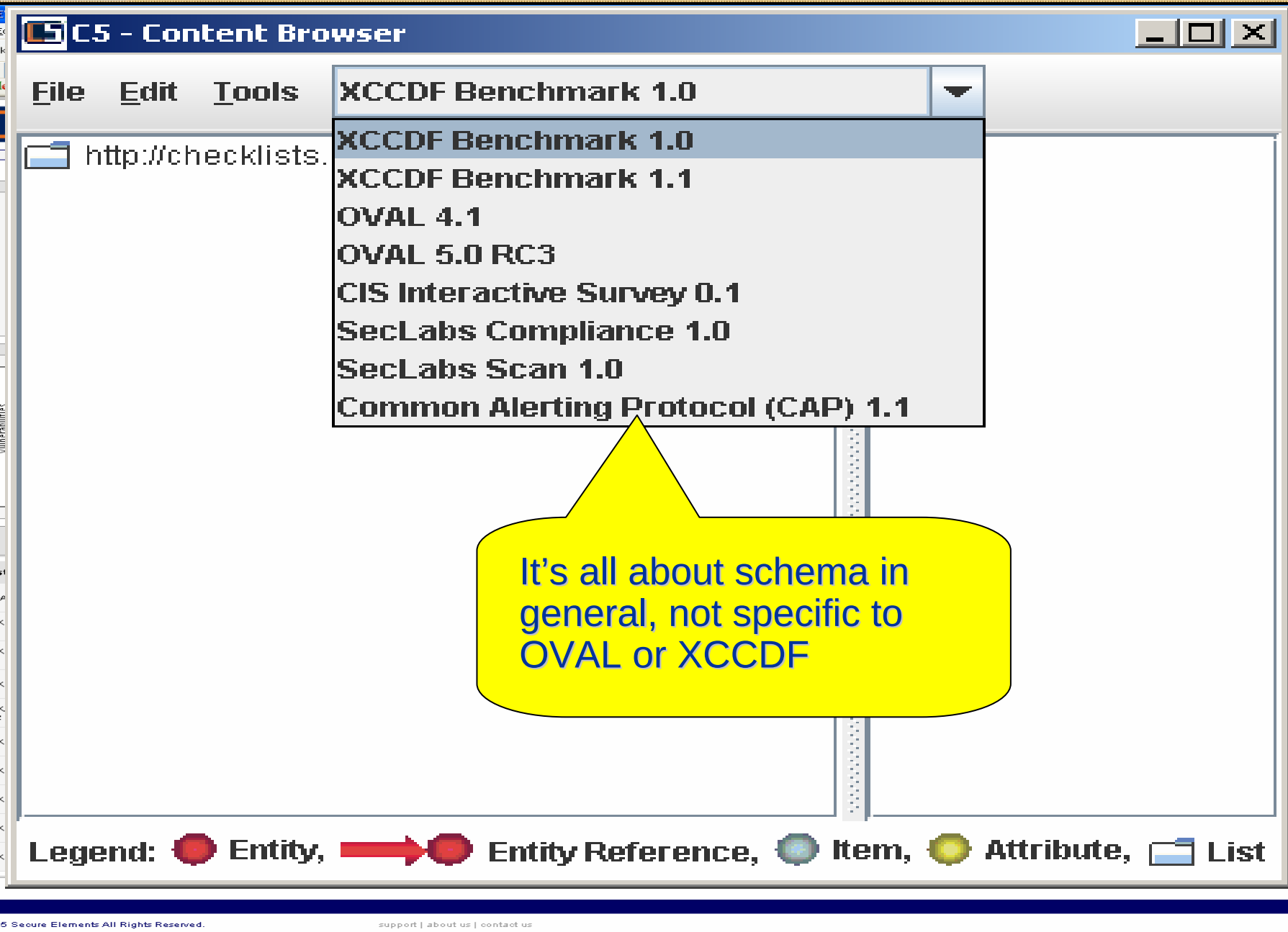
Host	IP Address	# of Vulns	OS type	OS version	Criticality	Status
SOJA-ORACLE	10.0.10.171	165	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Protected
W2K3SSP0O2K31-3	10.2.243.248	138	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Lowest	Protected
W2K3SSP0O2K31-2	10.2.232.235	132	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Medium	Protected
W2KPRO-SP4-VM2	10.2.251.221	118	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Disconnected
W2KASRV-SP4-VM2	10.2.251.230	77	Microsoft Windows 2000 Advanced Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KSRV-SP4-VM2	10.2.248.237	50	Microsoft Windows 2000 Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KPRO-SP3-VM3	10.2.231.229	49	Microsoft Windows 2000 Professional	Service Pack 3 (Build 2195)	Lowest	Protected
W2KPRO-SP2-VM2	10.2.254.213	46	Microsoft Windows 2000 Professional	Service Pack 2 (Build 2195)	High	Protected
W2KPRO-SP4-VM3	10.2.242.214	30	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	Low	Protected
W2KSRV-SP3-VM2	10.2.241.246	24	Microsoft Windows 2000 Server	Service Pack 3 (Build 2195)	Medium	Protected

Top 10 Unresolved Vulnerabilities (by # of occurrences)

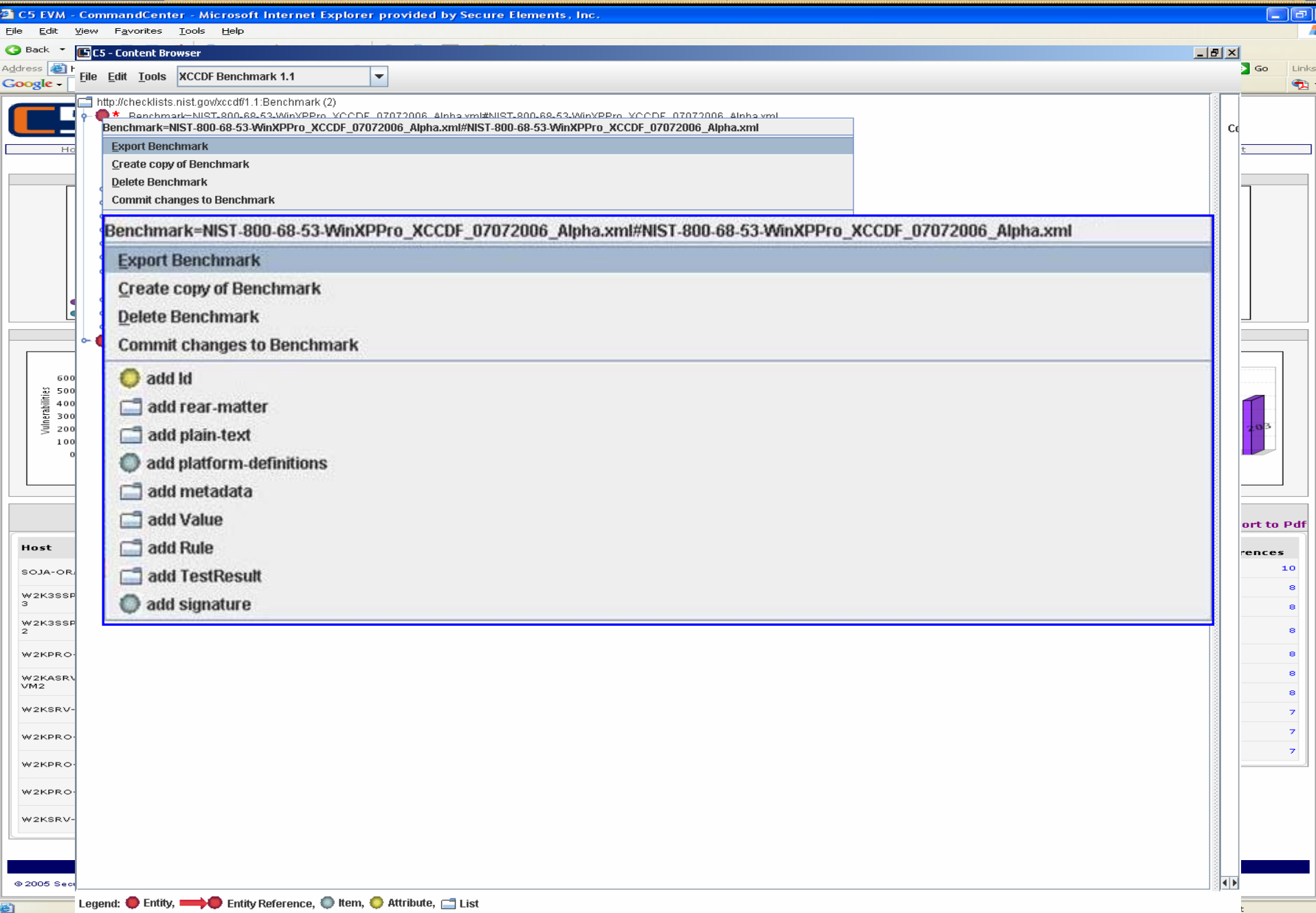
Export to Pdf

Vendor Id	Name	CVE/CAN Id	Severity	# of Occurrences
oval:org.mitre.oval:def:115	Hyperlink Object Function Vulnerability	CVE-2006-3438	High	10
oval:org.mitre.oval:def:13	Buffer Overrun in HTML Help Vulnerability	CVE-2006-3357	High	8
oval:org.mitre.oval:def:155	User Profile Elevation of Privilege Vulnerability	CVE-2006-3443	High	8
oval:org.mitre.oval:def:21	Microsoft Office Remote Code Execution Using a Malformed GIF Vulnerability	CVE-2006-0007	High	8
oval:org.mitre.oval:def:492	Buffer Overrun in Server Service Vulnerability	CVE-2006-3439	High	8
oval:org.mitre.oval:def:841	Unhandled Exception Vulnerability	CVE-2006-3648	High	8
oval:org.mitre.oval:def:1559	Windows Media Player Plug-in EMBED Vulnerability	CVE-2006-0005	Medium	8
oval:org.mitre.oval:def:723	DNS Client Buffer Overrun Vulnerability	CVE-2006-3441	High	7
oval:org.mitre.oval:def:747	Winsock Hostname Vulnerability	CVE-2006-3440	High	7
oval:org.mitre.oval:def:999	Hyperlink Object Buffer Overflow Vulnerability	CVE-2006-3086	High	7

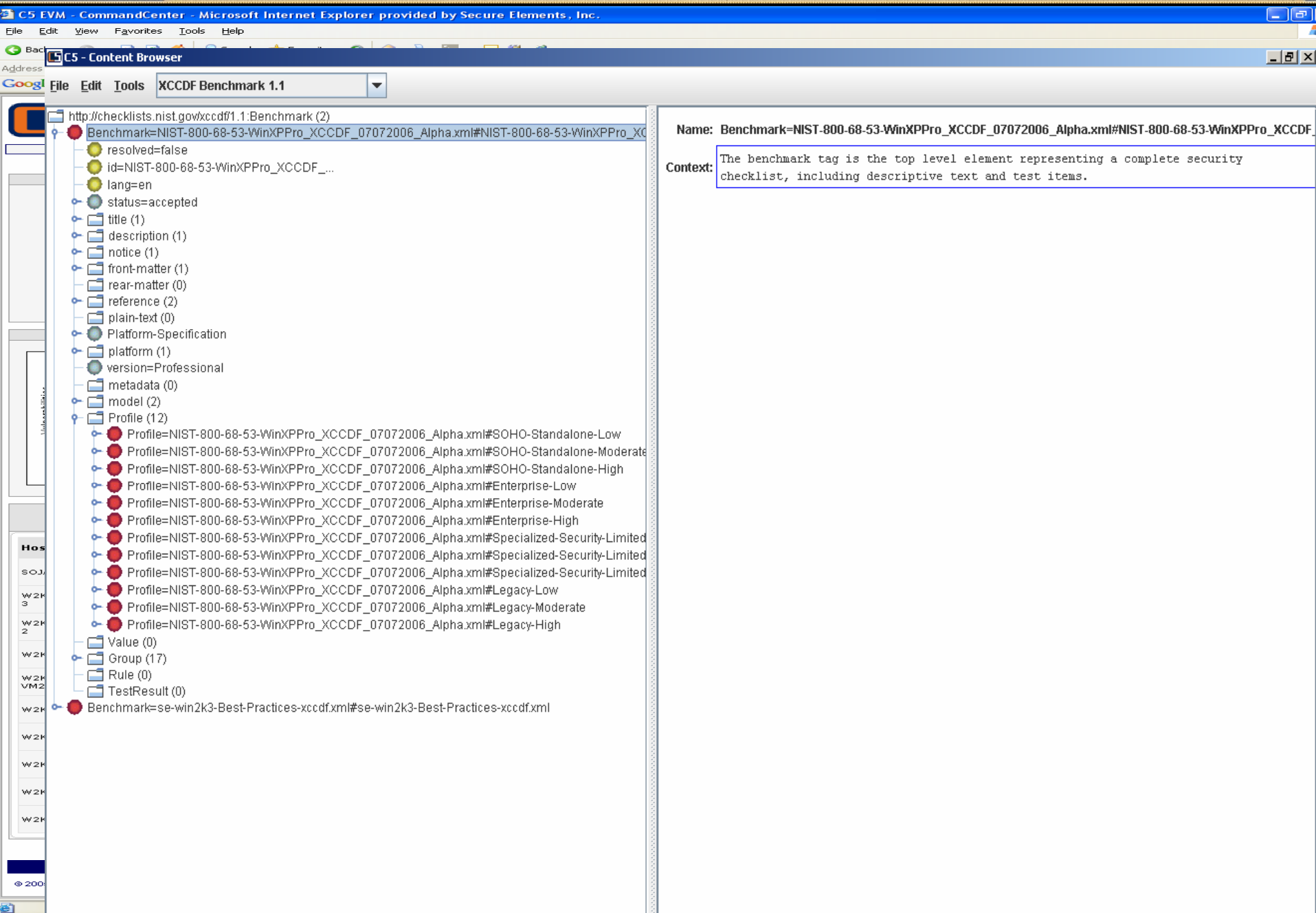
C5 Helium


C5 - Content Browser
File
Edit
Tools
XCCDF Benchmark 1.0
XCCDF Benchmark 1.0
XCCDF Benchmark 1.1
OVAL 4.1
OVAL 5.0 RC3
CIS Interactive Survey 0.1
SecLabs Compliance 1.0
SecLabs Scan 1.0
Common Alerting Protocol (CAP) 1.1
http://checklists.
It's all about schema in general, not specific to OVAL or XCCDF
Legend:
Entity,
Entity Reference,
Item,
Attribute,
List
© 2005 Secure Elements All Rights Reserved.
support | about us | contact us

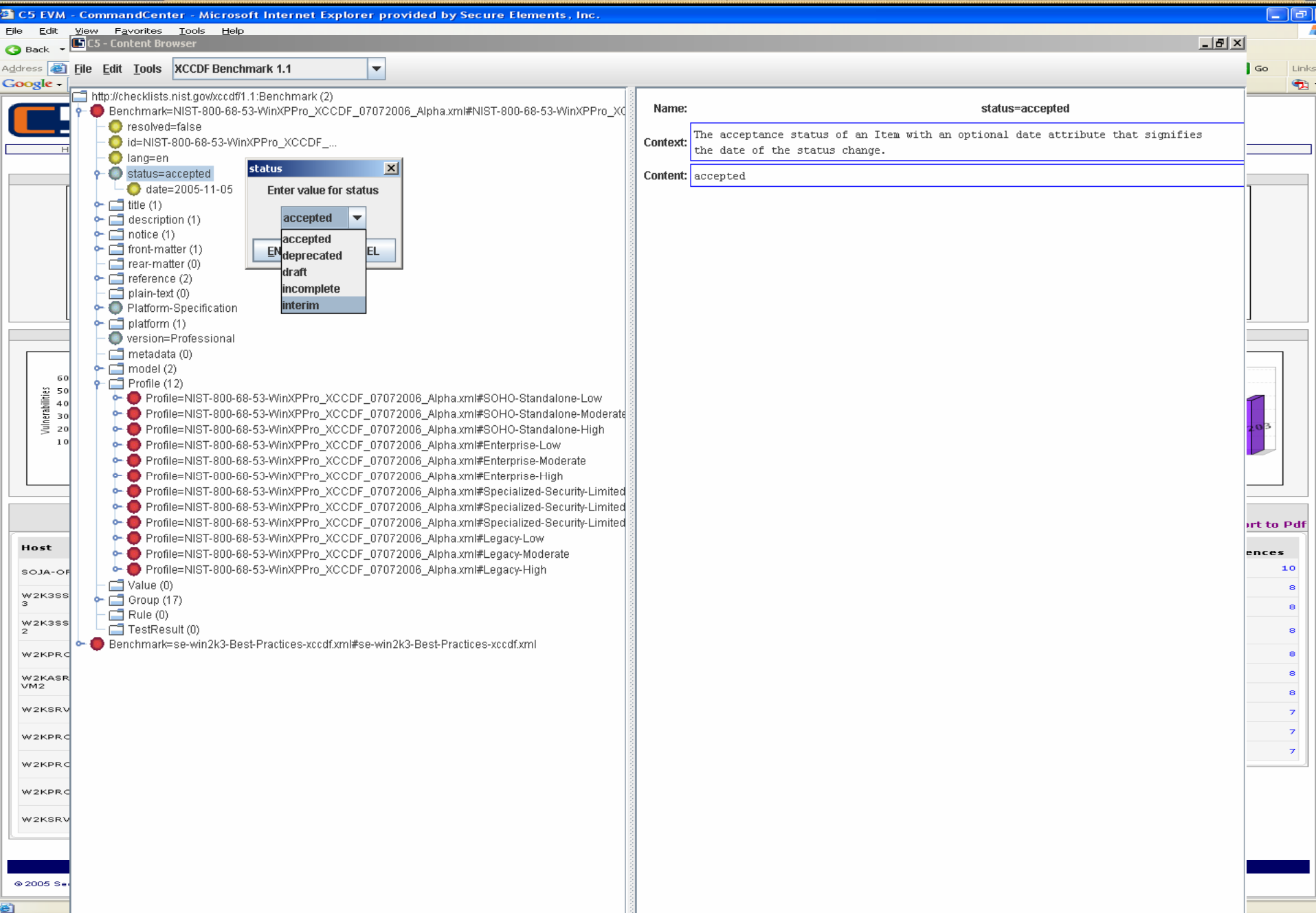
Schema Awareness



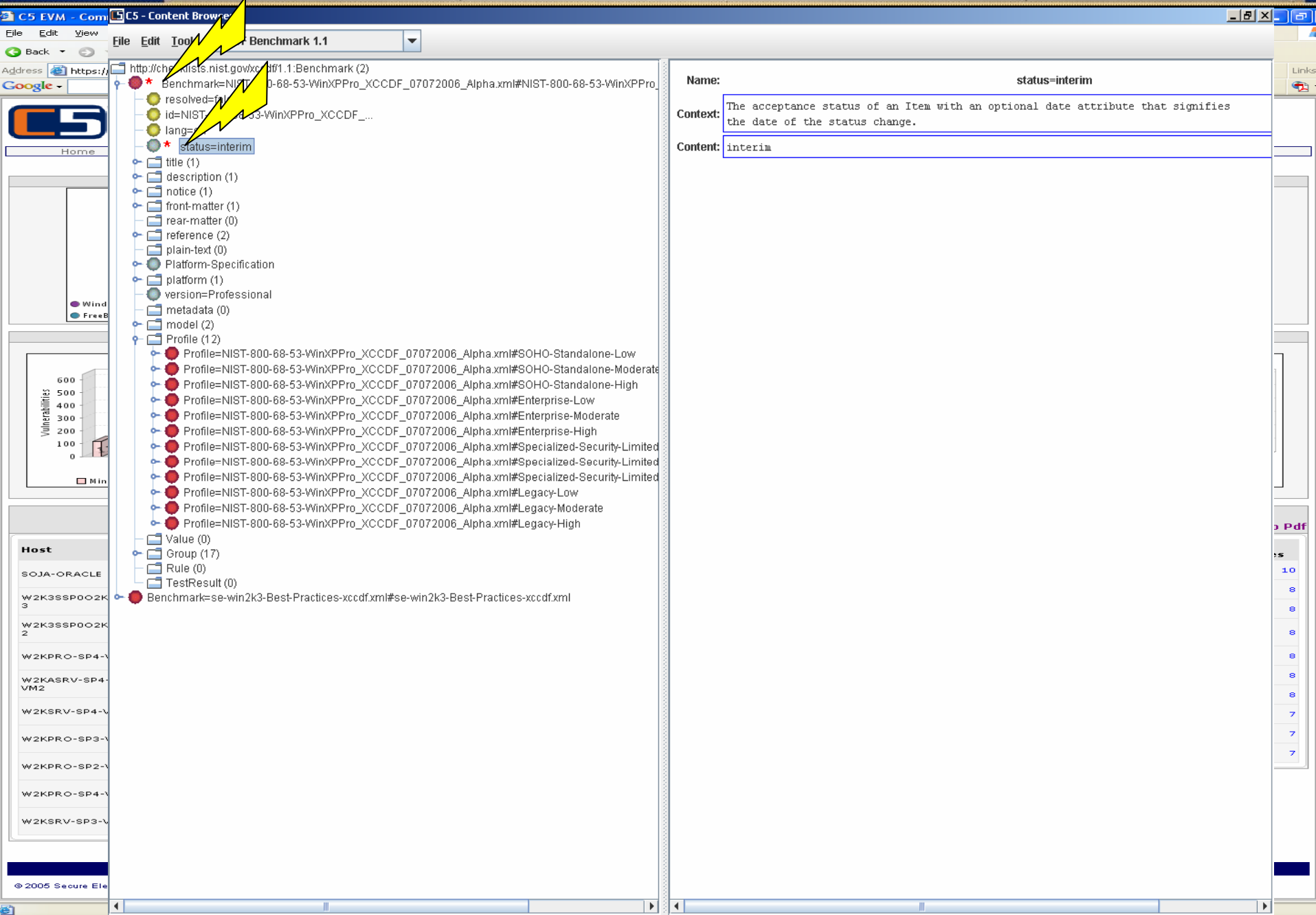
Profiles


C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.
File Edit View Favorites Tools Help
C5 - Content Browser
File Edit Tools XCCDF Benchmark 1.1
http://checklists.nist.gov/xccdf/1.1:Benchmark (2)
Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XC
resolved=false
id=NIST-800-68-53-WinXPPro_XCCDF_...
lang=en
status=accepted
title (1)
description (1)
notice (1)
front-matter (1)
rear-matter (0)
reference (2)
plain-text (0)
Platform-Specification
platform (1)
version=Professional
metadata (0)
model (2)
Profile (12)
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Moderate
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-High
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Low
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Moderate
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-High
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Low
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Moderate
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-High
Value (0)
Group (17)
Rule (0)
TestResult (0)
Benchmark=se-win2k3-Best-Practices-xccdf.xml#se-win2k3-Best-Practices-xccdf.xml
Name: Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_
Context: The benchmark tag is the top level element representing a complete security checklist, including descriptive text and test items.

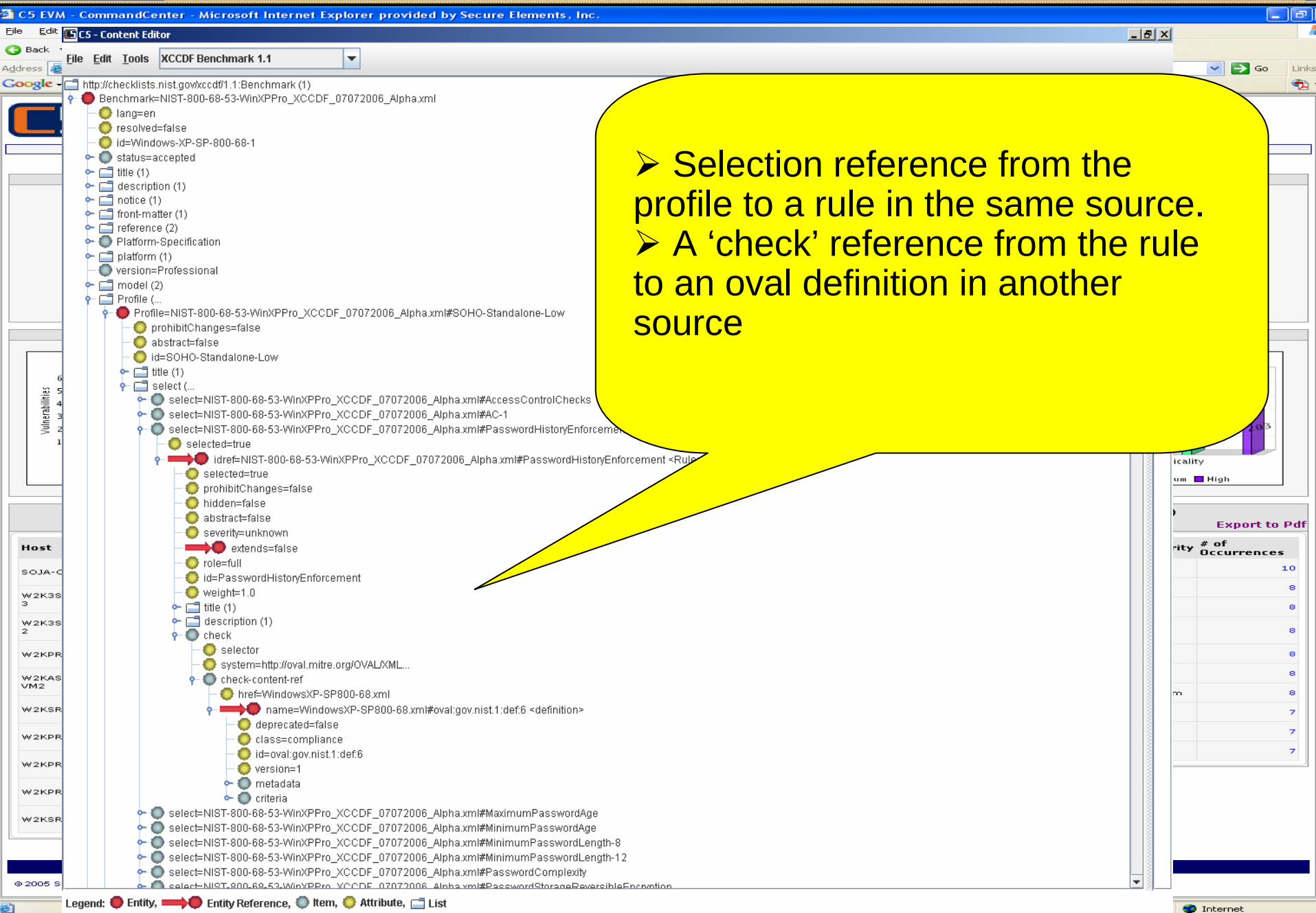
Simple Editing



Editing

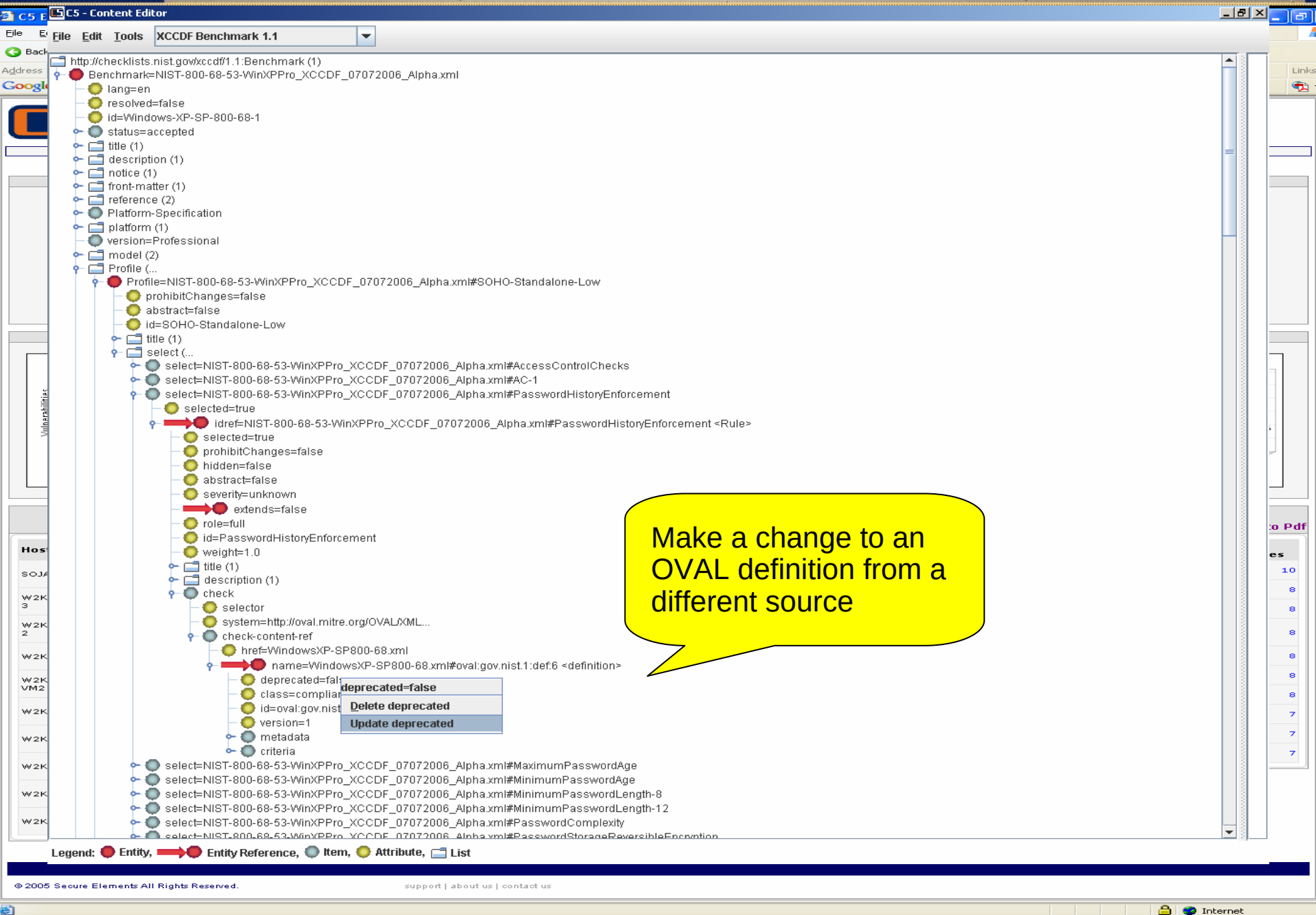

C5 - Content Browser
File Edit Tools Benchmark 1.1
http://checklists.nist.gov/xccdf/1.1:Benchmark (2)
Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_
resolved=false
id=NIST-800-68-53-WinXPPro_XCCDF_...
lang=en
status=interim
title (1)
description (1)
notice (1)
front-matter (1)
rear-matter (0)
reference (2)
plain-text (0)
Platform-Specification
platform (1)
version=Professional
metadata (0)
model (2)
Profile (12)
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Moderate
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-High
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Low
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Moderate
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-High
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Low
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Moderate
Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-High
Value (0)
Group (17)
Rule (0)
TestResult (0)
Benchmark=se-win2k3-Best-Practices-xccdf.xml#se-win2k3-Best-Practices-xccdf.xml
Name: status=interim
Context: The acceptance status of an Item with an optional date attribute that signifies the date of the status change.
Content: interim

Inter-Source Updating



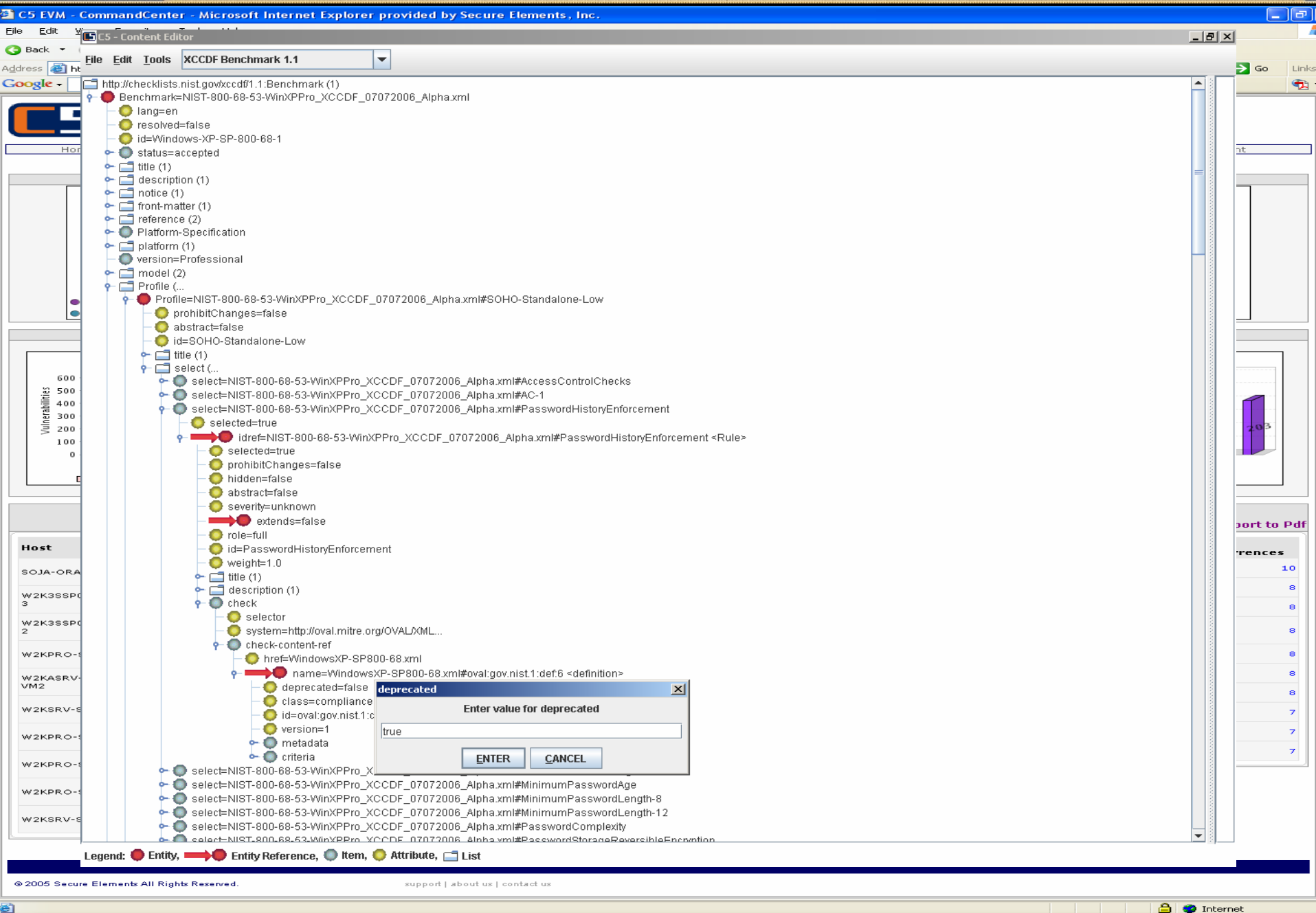
- Selection reference from the profile to a rule in the same source.
- A ‘check’ reference from the rule to an oval definition in another source

Inter-Source Updating

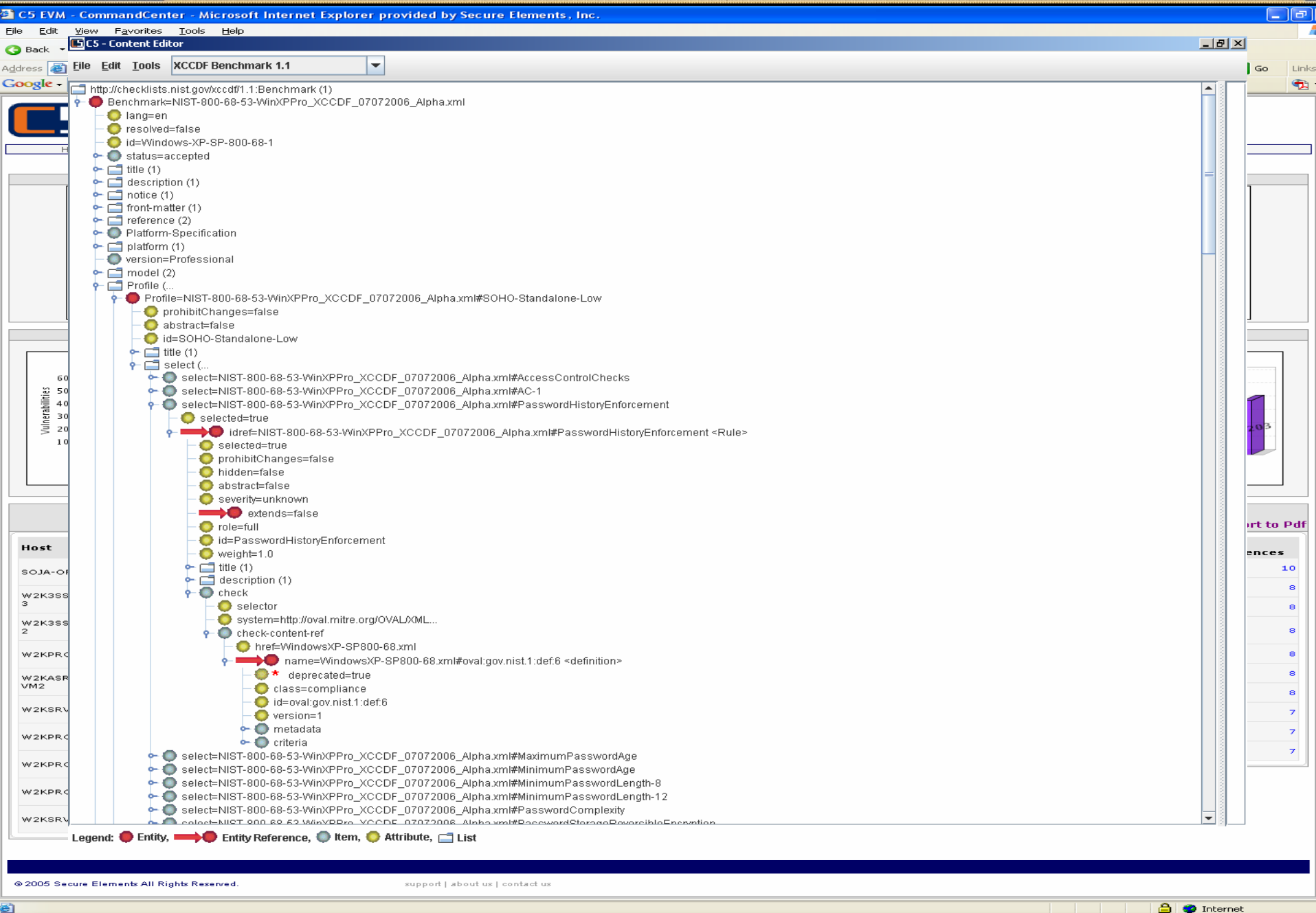


Make a change to an OVAL definition from a different source

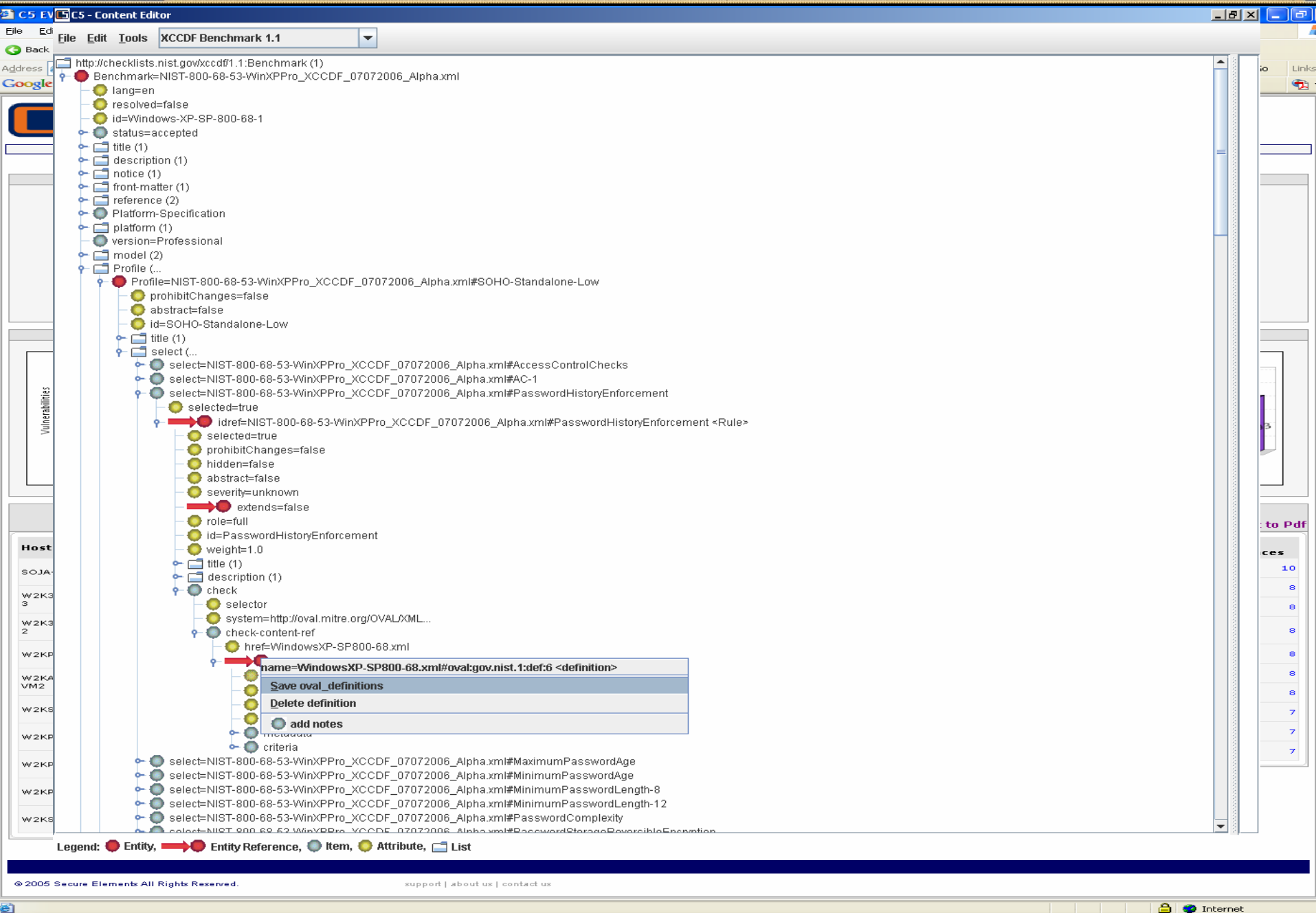
Inter-Source Updating



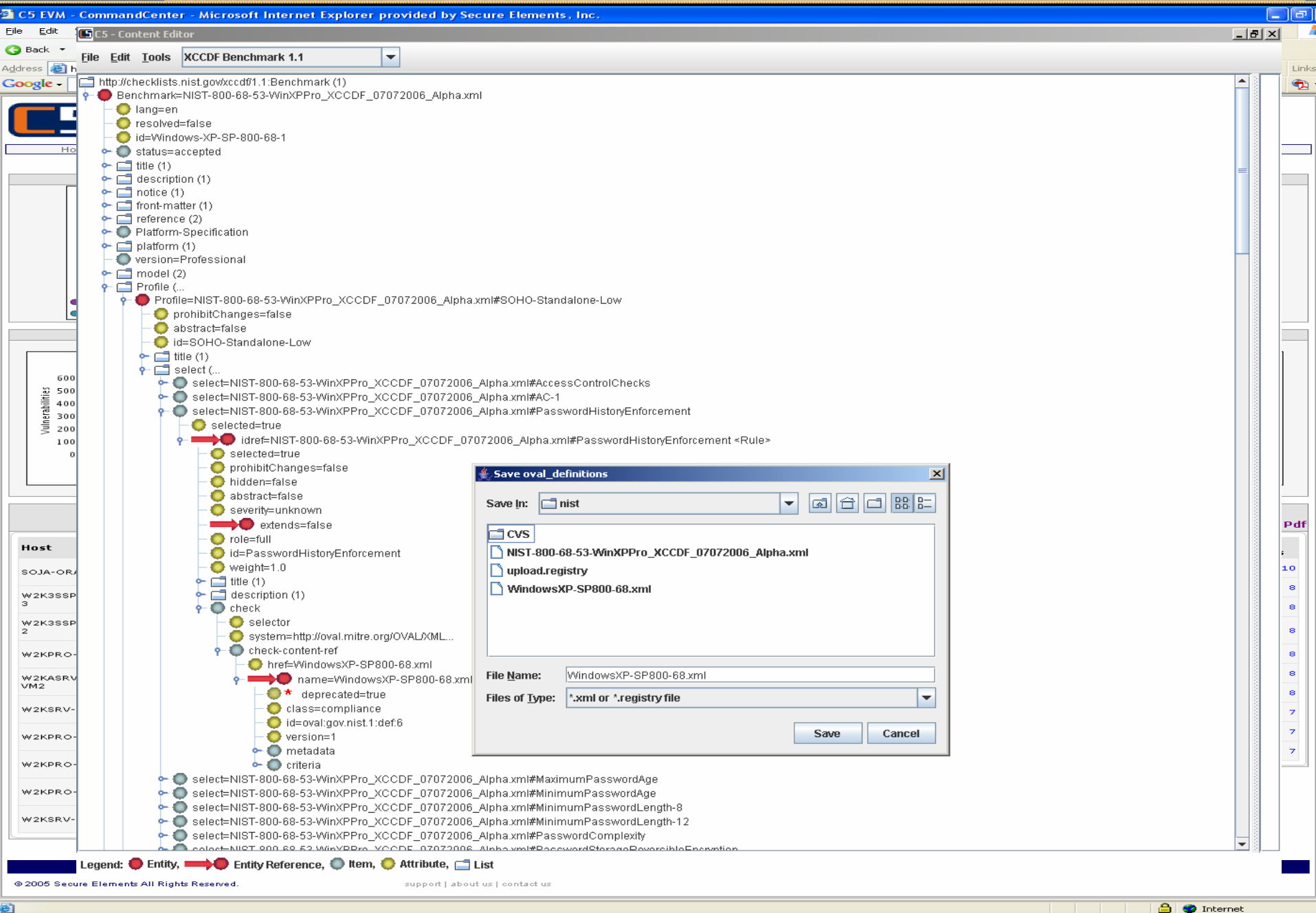
Inter-Source Updating



Inter-Source Updating



Inter-Source Updating



secure elements®

Audit. Evaluate. Comply.

"It really is that simple"

Questions?